

Wachendorff Prozesstechnik GmbH & Co. KG
Industriestrasse 7
D-65366 Geisenheim
Tel.: +49 (0) 67 22 / 99 65 - 20
Fax: +49 (0) 67 22 / 99 65 - 78
www.wachendorff-prozesstechnik.de

Wireless Access Point

WLANAP0C

Benutzerhandbuch



Version 1.3



Inhalt



1. Vorwort

Verehrter Kunde!
Wir bedanken uns für Ihre Entscheidung ein Produkt unseres Hauses einzusetzen und gratulieren Ihnen zu diesem Entschluss. Das Gerät kann vor Ort für zahlreiche unterschiedliche Anwendungen eingesetzt werden.
Um die Funktionsvielfalt dieses Gerätes für Sie optimal zu nutzen, bitten wir Sie folgendes zu beachten:
Jede Person, die mit der Inbetriebnahme oder Bedienung dieses Gerätes beauftragt ist, muss die Betriebsanleitung und insbesondere die Sicherheitshinweise gelesen und verstanden haben!

2. Sicherheitshinweise

2.1. Allgemeine Hinweise



Zur Gewährleistung eines sicheren Betriebes darf das Gerät nur nach den Angaben in der Betriebsanleitung betrieben werden. Bei der Verwendung sind zusätzlich die für den jeweiligen Anwendungsfall erforderlichen Rechts- und Sicherheitsvorschriften zu beachten. Sinngemäß gilt dies auch bei Verwendung von Zubehör.

2.2. Bestimmungsgemäße Verwendung

Das Gerät dient als Access Point zur WLAN-Verbindung mit einem Client. Jeder darüber hinausgehende Gebrauch gilt als nicht bestimmungsgemäß.



Dieses Gerät darf nicht als alleiniges Mittel zur Abwendung gefährlicher Zustände an Maschinen und Anlagen eingesetzt werden. Maschinen und Anlagen müssen so konstruiert werden, das fehlerhafte Zustände nicht zu einer für das Bedienpersonal gefährlichen Situation führen können (z. B. durch unabhängige Grenzwertschalter, mechanische Verriegelungen, etc.).

2.3. Qualifiziertes Personal

Dieses Gerät darf nur von qualifiziertem Personal, ausschließlich entsprechend der technischen Daten verwendet werden.
Qualifiziertes Personal sind Personen, die mit der Aufstellung, Montage, Inbetriebnahme und Betrieb dieses Gerätes vertraut sind und die über eine ihrer Tätigkeit entsprechenden Qualifikation verfügen.

2.4. Restgefahren

Dieses Gerät entspricht dem Stand der Technik und ist betriebssicher. Von dem Gerät können Restgefahren ausgehen, wenn sie von ungeschultem Personal unsachgemäß eingesetzt und bedient werden.
In dieser Anleitung wird auf Restgefahren mit dem folgenden Symbol hingewiesen:



Dieses Symbol weist darauf hin, dass bei Nichtbeachtung der Sicher- heitshinweise Gefahren für Menschen bis zur schweren Körperverletzung oder Tod und/oder die Möglichkeit von Sachschäden besteht.



2.5. CE-Konformität

Die Konformitätserklärung liegt bei uns aus. Sie können diese gerne beziehen. Nehmen Sie einfach Kontakt mit uns auf.

3. Copyright

4. Sonstige Bestimmungen und Standards

FCC Bedingungen



Dieses Gerät wurde getestet und entspricht Teil 15, Klasse B der FCC-Bestimmungen. Der Betrieb unterliegt den beiden folgenden Bedingungen:
(1) Dieses Gerät darf keine schädlichen Störungen verursachen.
(2) Dieses Gerät muss jede empfangene Störung akzeptieren und diese beinhalten Störungen, die durch unerwünschten Betrieb verursacht werden.

WEEE Informationen



Entsorgung von alten Elektro- und Elektronikgeräten (gültig in der Europäischen Union und anderen europäischen Ländern mit separatem Sammelsystem)
Dieses Symbol auf dem Produkt oder auf der Verpackung bedeutet, dass dieses Produkt nicht wie Hausmüll behandelt werden darf. Stattdessen soll dieses Produkt zu dem geeigneten Entsorgungspunkt zum Recyceln von Elektro- und Elektronikgeräten gebracht werden. Wird das Produkt korrekt entsorgt, helfen Sie mit, negativen Umwelteinflüssen und Gesundheitsschäden vorzubeugen, die durch unsachgemäße Entsorgung verursacht werden könnten. Das Recycling von Material wird unsere Naturressourcen erhalten. Für nähere Informationen über das Recyceln dieses Produktes kontaktieren Sie bitte Ihr lokales Bürgerbüro, Ihren Hausmüll Abholservice oder das Geschäft, in dem Sie dieses Produkt gekauft haben.

FCC-WARNUNG

Klasse B für dieses Produkt

Dieses Produkt wurde geprüft und entspricht den Grenzwerten für digitale Geräte der Klasse B gemäß Abschnitt 15 der FCC-Richtlinien (Federal Communications Commission: US-amerikanische Regulierungsbehörde). Diese Grenzwerte wurden festgelegt, um einen angemessenen Schutz gegen schädliche Störungen im privaten Gebrauch zu bieten. Dieses Gerät erzeugt und verwendet Radiofrequenzenergie und kann diese ausstrahlen. Es kann, wenn es nicht gemäß den Anweisungen installiert und betrieben wird, schädliche Funkverkehrsstörungen verursachen. Es kann jedoch nicht garantiert werden, dass es bei einer bestimmten Installation nicht doch zu einer Störung kommt. Sollte dieses Gerät schädliche Störungen im Funk- und Fernsehempfang verursachen (feststellbar durch Ein- und Ausschalten des Geräts), sollten Sie versuchen, die Störung durch eine der folgenden Maßnahmen zu beheben:

- Richten Sie die Empfangsantenne anders aus, oder bringen Sie sie an einer anderen Stelle an.
- Vergrößern Sie den Abstand zwischen dem Gerät und dem Empfänger.



- Schließen Sie das Gerät an eine Steckdose eines anderen Stromkreises als den des Empfängers an.
- Wenden Sie sich an Ihren Händler oder einen erfahrenen Radio- und Fernsehtechniker.

Dieses Produkt entspricht Teil 15 der FCC-Richtlinien. Der Betrieb ist nur zulässig, wenn die beiden folgenden Bedingungen erfüllt sind: (1) Dieses Gerät verursacht keine gefährlichen Störungen und (2) dieses Gerät muss empfangene Störungen verarbeiten können, einschließlich solcher Störungen, die einen unerwünschten Betrieb verursachen können.

FCC-Warnung: Änderungen oder Modifikationen, die nicht ausdrücklich von der zuständigen Stelle genehmigt worden sind, können dazu führen, dass der Benutzer die Betriebserlaubnis für dieses Gerät verliert.

WICHTIGER HINWEIS:

FCC-Strahlenbelastungserklärung:

Dieses Produkt hält die von der FCC vorgegebenen Strahlenbelastungsgrenzwerte für nicht kontrollierte Umgebungen ein. Dieses Produkt muss mindestens 20 cm vom Anwender entfernt installiert und betrieben werden. Dieses Produkt darf nicht zusammen mit einer anderen Antenne oder einem anderen Sender aufgestellt oder betrieben werden. Die verfügbaren Kanäle für den Betrieb dieses Produkts mit 802.11 b/g in den USA sind die Kanäle 1 bis 11. Die Kanalauswahl wird durch die Firmware beschränkt.

UL-Hinweis für Spannungsversorgung

Die Produktreihe WLANxxxx wird mit einem mit „LPS“ (Limited Power Source) oder „Class 2“ gekennzeichneten Netzteil mit einer Ausgangsleistung von mindestens 9~48 VDC, 1,0 A geliefert oder Sie verwenden das empfohlene Netzteil, das in den „Bestellhinweisen“ S. 57 angegeben ist.

5. Einführung

5.1. Produktübersicht

Der Wireless Access Point WLANAP0C gehört zu unserer Wireless-Produktlinie, die drahtlose Konnektivität für Wireless Clients bzw. Mobilstationen bereitstellen und damit komplett mobile und drahtlose Netze für Ihre industriellen Netzwerke schaffen. Sie können beispielsweise WLAN-Clients mit dem Wireless Access Point WLANAP0C verbinden. Damit können andere Geräte in ein lokales Netzwerk (LAN) oder ein Backbone-Netz eingebunden werden. Der Wireless Access Point WLANAP0C unterstützt mobile und drahtlose Netzwerke durch mehrere Funktionalitäten. Der WLANAP0C unterstützt kein Profinet.

WLANAP0C unterstützt drei Betriebsarten:

- Access-Point-Betrieb
- Wireless-Bridge-Betrieb
- „AP + Wireless Bridge“-Betrieb

5.2. Funktionen

Der Wireless Access Point WLANAP0C verfügt über die nachstehend angeführten Funktionen.

- o Drahtloses Netzwerk mit Standard IEEE 802.11b/g, 54Mbps



- Firewall und Paketfilterung
- Sicherheit der drahtlosen Verbindung: Open, WEP, WPA-PSK, WPA2-PSK, WPA, WPA2, IEEE 802.1x/RADIUS
- Wireless-Bridge-Sicherheit: Open, WEP, TKIP, CCMP(AES) Verschlüsselungsalgorithmus
- Metallgehäuse (Schutzklasse IP 50).
- Betriebstemperatur: 0 bis 60° C
- Lagertemperatur: -40 bis 70° C
- 15kV ESD-Schutz für serielle Ports
- Konfiguration über Webserver
- Optionale 2,4 GHz-Standardantenne mit hohem Gewinn
- Firmware kann über Netzwerkanschluss aktualisiert werden

6. Erste Schritte

6.1. Inhalt des Pakets

- Ein Wireless Access Point WLANAP0C für Industrieanwendungen
- Eine 2 dBi Demo-Whip Antenne
- Zwei Bausätze zur Wandmontage

ANMERKUNG: Benachrichtigen Sie unverzüglich Ihren Lieferanten, wenn bei der Anlieferung einer der oben genannten Artikel fehlt oder beschädigt ist.



6.2. Vorder- und Rückseiten

SMA-Antennenanschluss

LED-Anzeige für AP-Betrieb

LED-Anzeige LAN-Aktivität

LED-Anzeige Wireless-Aktivität

10/100Mbps Ethernet-Port

Resetknopf zur Wiederherstellung der Werkseinstellungen

LED-Anzeige für Wireless- Bridge-Verbindungen

LED-Anzeige für Wireless Bridge & AP Verbindungen

LED-Anzeige (reserviert)

LED-Anzeige für Systemstatus und Strom EIN

3-polige Klemmleiste für Stromversorgung

WLANAP0C Vorderseite

6.3. Erstinstallation

- Bereiten Sie die erforderlichen Kabel, Netzteile und Kabel vor.
- Schrauben Sie die Antenne an dem SMA-Antennenanschluss an.
- Stellen Sie den WLANAP0C am gewünschten Standort auf und schließen Sie ihn über das Ethernetkabel mit dem RJ45-Stecker ans LAN an.
- Verbinden Sie den WLANAP0C (mit dem Netzstecker oder dem 3-poligen Klemmleistenstecker) mit einer 9 bis 48 VDC Stromquelle.
- Wenn der WLANAP0C richtig angeschlossen wurde, ertönt ein Summersignal und die RUN-LED blinkt. Informationen zum LED-Status finden Sie in Kapitel 5.
- Schließen Sie Ihren Computer ans LAN an. Als Standardkonfiguration des WLANAP0C ist die Betriebsart „Access Point“ mit der festen IP-Adresse 10.0.50.200 und dem Standard-Gateway 10.0.50.1 eingestellt. Unter http://10.0.50.200 können Sie auf die Webkonfiguration des WLANAP0C zugreifen. Informationen zu weiteren Einstellungen finden Sie im nächsten Abschnitt.

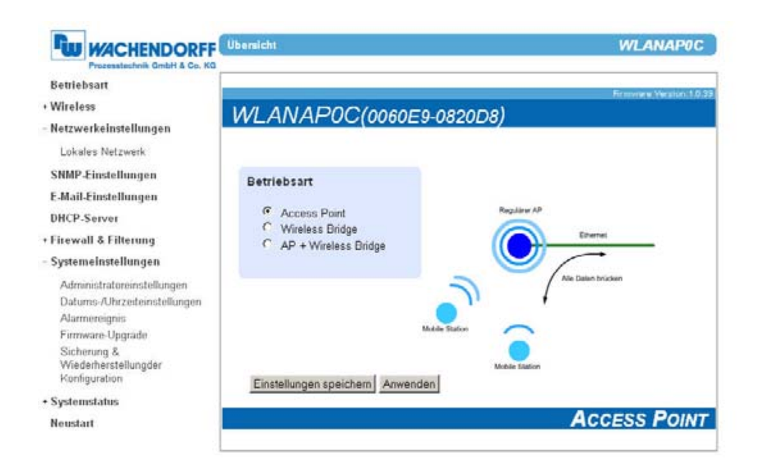




Anschließen der Antenne und der Kabel an das Gerät

6.3.1. Übersicht über die Webkonfiguration

Die Webkonfiguration des WLANAP0C ist für eine einfache Konfiguration zur Anpassung an die Kundenbedürfnisse in drei Prozessschritte unterteilt. Die Webkonfigurationsseite ist aus zwei Frames aufgebaut. Der linke Frame ist der Menüframe und der rechte Frame ist der Hauptkonfigurationsframe.



Übersicht über die Webkonfiguration

- Der Inhalt des Menüframes hängt von der eingestellten Betriebsart des Geräts ab. Beispielsweise beinhalten die Menüpunkte der Wireless-Einstellungen in der Betriebsart „Wireless Bridge" den zusätzlichen Menüpunkt „Wireless-Bridge-Schnittstelle".
- Der Inhalt des Hauptkonfigurationsframes hängt von dem Menüpunkt ab, der im oben aufgeführten Menüframe ausgewählt wird.
- Die Konfigurationsframes verfügen über drei Hauptschaltflächen.



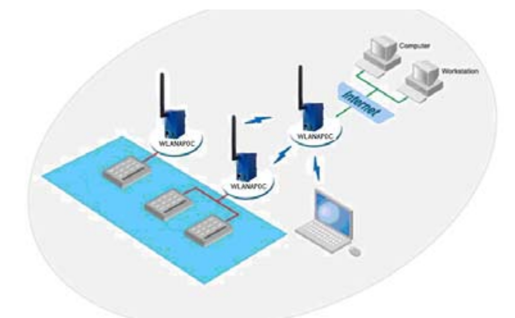
Schaltfläche	Funktionalität
Einstellungen speichern	Aktuelle Konfigurationseingabe nur auf der Seite speichern. Die Konfiguration findet keine Anwendung auf dem Gerät. Wir empfehlen den Benutzern, diese Schaltfläche zu verwenden, bevor die Konfiguration abgeschlossen ist und als letzten Schritt auf die Schaltfläche „Anwenden (Apply)“ zu klicken.
Anwenden	Aktuelle Konfigurationseingabe auf der Seite speichern und anwenden. Auf einigen Seiten muss das Gerät unter Umständen neu gestartet werden.
Abbruch	Aktuelle Konfigurationseingabe löschen und die ursprünglichen Einstellungen anzeigen.

6.3.2. Anleitung zur Auswahl der Betriebsart des WLANAP0C

In diesem Abschnitt geben wir einen Überblick über die verschiedenen Betriebsarten des WLANAP0C und führen für jede Betriebsart einige Netzwerktopologiebeispiele an.

Access-Point-Betrieb

Im Access-Point-Betrieb agiert der WLANAP0C als Wireless-Access-Point, der alle Wireless-Clients auf seiner LAN-Schnittstelle mit einem kabelgebundenen Ethernet-Netz verbindet. Er agiert als Bridge zwischen Wireless-Schnittstelle und Ethernet-Schnittstelle. Das Gerät fügt die drahtlosen und die kabelgebundenen Netze in transparenter Weise zu einem einzigen Netz zusammen.



Topologiebeispiel für den WLANAP0C im AP-Betrieb

Wireless-Bridge-Betrieb

In dieser Betriebsart unterstützt der WLANAP0C die drahtlose Verbindung zwischen Access Points. Er agiert als Verbindung zwischen den physisch getrennten Ethernet-Netzwerken seiner



angeschlossenen WLANAP0C-Geräte. Es sind maximal vier gleichzeitige Wireless-Bridge-Anschlüsse möglich. Indem wir in jedem Ethernet-Netz einen WLANAP0C im Wireless-Bridge-Betrieb installieren, können wir alle kabelgebundenen Ethernet-Teilnehmer auf den LAN-Schnittstellen dieser Geräte zu einem einzigen Ethernet-Netz verbinden. Beachten Sie, dass diese Betriebsart nur mit anderen WLANAP0C-Geräten funktioniert.

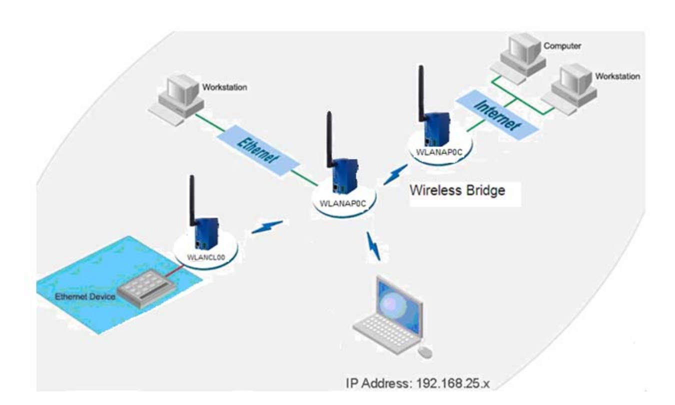


Topologiebeispiel für den WLANAP0C im Wireless-Bridge-Betrieb

AP + Wireless Bridge

In dieser Betriebsart agiert der WLANAP0C sowohl als Wireless Access Point als auch als Wireless Bridge. Er verbindet Wireless Clients und kabelgebundene Clients auf seiner LAN-Schnittstelle und fügt sie über den Wireless-Bridge-Anschluss mit dem Netz seiner angeschlossenen WLANAP0C-Geräte zusammen. Es sind maximal vier gleichzeitige Wireless-Bridge-Anschlüsse möglich. Beachten Sie, dass diese Betriebsart nur mit anderen WLANAP0C-Geräten funktioniert.

Indem wir in jedem Netz einen WLANAP0C im Betrieb „AP + Wireless Bridge“ installieren, können wir alle kabelgebundenen Clients und Wireless Clients auf den LAN- und WLAN-Schnittstellen dieser Geräte in transparenter Weise zu einem einzigen Netz verbinden.



Topologiebeispiel für den WLANAP0C im „AP + Wireless-Bridge“-Betrieb



6.4. Werkseinstellungen

Der WLANAP0C verfügt über zwei Netzwerk-Schnittstellen, Ethernet und drahtlose Netzwerkschnittstellen. Nachstehend sind die Standardeinstellungen der beiden Schnittstellen sowie Benutzername und Passwort für die Erstinstallation angeführt.

Standard-IP-Adressen		
Schnittstelle	**Geräte-IP**	**Subnetzmaske**
Ethernetport	10.0.50.200	255.0.0.0
Benutzername	admin	
Passwort	(Leer)	

Weitere Standardeinstellungen sind in der folgenden Tabelle angegeben.

<u>**Anmerkung**</u> **Parameter, die mit † markiert sind, sind lediglich im Wireless-Bridge-Betrieb verfügbar.**

Tabelle: Werkseinstellungen

Parameter	Standardwerte
Überblick	
Betriebsart	Access Point
Wireless	
Grundeinstellung: SSID	WLANAP0C
Grundeinstellung: Kanal	Automatikbetrieb
Grundeinstellung: SSID-Broadcast	Aktiviert
Grundeinstellung: Wireless-Modus	802.11b/g GEMISCHT
Sicherheitseinstellungen: Authentifizierungsmodus	Deaktiviert
Sicherheitseinstellungen: Verschlüsselungsart	KEINE
Wireless-Bridge-Schnittstelle: Verschlüsselungsart	KEINE
Wireless-Bridge-Schnittstelle: Passphrasen-Schlüssel	(LEER)
Wireless-Bridge-Schnittstelle: Wireless-Bridge-Schnittstellenliste	(Nicht eingestellt)
Erweiterte Einstellungen: Land Region	US (Kanal 1-11)
Erweiterte Einstellungen: Landescode	US (UNITED STATES)
Erweiterte Einstellungen: Übertragsungsrate	Automatikbetrieb
Erweiterte Einstellungen: Grundrate	15 Mbps
Erweiterte Einstellungen: Beacon-Periode	100 Millisekunden
Erweiterte Einstellungen: DTIM-Periode	3 Millisekunden
Erweiterte Einstellungen: Tx Power [Sendeleistung]	100%



Erweiterte Einstellungen: Fragmentierungsschwelle	2346 Bytes
Erweiterte Einstellungen: RTS-Schwelle	2347 Bytes
Netzwerkeinstellungen	
LAN: DHCP (Obtain an IP Address Automatically [IP-Adresse automatisch beziehen])	Deaktiviert
LAN: IP-Adresse	10.0.50.200
LAN: Subnetzmaske	255.0.0.0
LAN: Standard-Gateway	10.0.50.1
LAN: Bevorzugter DNS	168.95.1.1
LAN: Alternativer DNS	(Leer)
SNMP-Einstellungen	
Systemansprechpartner	Ansprechpartner
Systemname	Name
Systemstandort	Standort
SNMP-Dienst	Deaktiviert
Read-Community	public
Write-Community	private
SNMP-Trap-Server	0.0.0.0
E-Mail-Einstellungen	
Sender	(Leer)
Empfänger	(Leer)
SMTP-Server	(Leer)
Authentifizierung	Deaktiviert
Benutzername	(Leer)
Passwort	(Leer)
DHCP-Server	
DHCP	Deaktiviert
Von IP-Adresse	(Leer)
Zu IP-Adresse	(Leer)
Netzmaske	(Leer)
Lease-Time (Minuten)	21600
Statischer Anschluss	(Nicht eingestellt)
Firewall und Filterung	
MAC-Filterung (kabelgebunden)	Deaktiviert
Ethernet-Filterung	Deaktiviert
IP-Filterung	Deaktiviert



Systemeinstellungen	
Benutzername	admin
Passwort	(LEER)
Datum-/Uhrzeiteinstellungen: NTP (Datum und Uhrzeit werden automatisch über das Netz synchronisiert)	Deaktiviert
Datum-/Uhrzeiteinstellungen: NTP-Server	pool.ntp.org
Datum-/Uhrzeiteinstellungen: Zeitzone	GMT
Manuelle Zeiteinstellungen: Datum	1. Januar 2006
Manuelle Zeiteinstellungen: Uhrzeit	0:00:00
Alarmereignis: Kaltstart	Deaktiviert
Alarmereignis: Warmstart	Deaktiviert
Alarmereignis: Authentifizierungsfehler	Deaktiviert
Alarmereignis: IP-Adresse geändert	Deaktiviert
Alarmereignis: Passwort geändert	Deaktiviert
Trap-Alarm: Kaltstart	Deaktiviert
Trap-Alarm: Warmstart	Deaktiviert
Trap-Alarm: Authentifizierungsfehler	Deaktiviert

ANMERKUNG: **Die Werkseinstellungen des Geräts können wiederhergestellt werden, indem der Resetknopf auf der Vorderseite mit einer Büroklammer fünf Sekunden lang gedrückt wird.**

Sie können das Gerät auch über die Konfiguration der Webkonsole neu starten bzw. auf die Werkseinstellungen zurückstellen.



7. Grundeinstellungen

In diesem Kapitel werden die Schritte zum Vornehmen der Grundeinstellungen und die Konfigurationsabläufe für jeden Betriebsmodus angeführt.

Wir unterteilen die Anweisungen in die folgenden 6 Schritte.

Schritt 1: Administrator-Login

Schritt 2: Betriebsart des Geräts

Schritt 3: Konfiguration des drahtlosen Netzwerks

Schritt 4: Netzwerk-Konfiguration

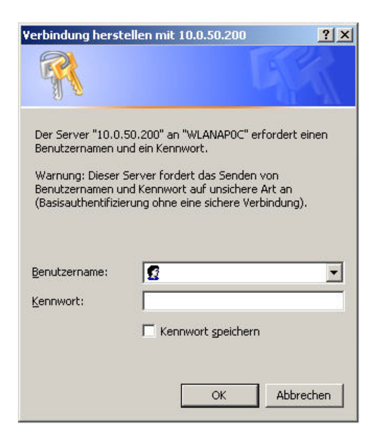
Schritt 5: Administrator-Passwort ändern

Schritt 6: Firmware aktualisieren (Optional)

7.1. Administrator-Login

Geben Sie im Web-Browser, beispielsweise Microsoft Internet Explorer oder Mozilla Firefox auf der URL die IP-Adresse des Geräts ein. ***Beispiel:*** *http://10.0.50.200* oder *http://your-device-IP*.

Es öffnet sich der Authentifizierungs-Bildschirm. Geben Sie den Benutzernamen und Passwort ein und klicken Sie anschließend auf „OK". Der Standard-Benutzername ist „admin" und das Passwort ist Null (lassen Sie es leer).

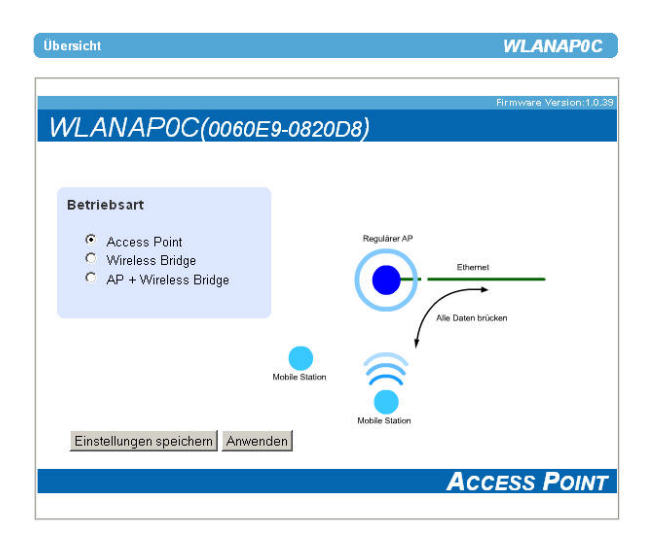


Authentifizierungsdialog zum Administrator-Login

7.2. Betriebsart des Geräts

Sobald sich der Administrator anmeldet, öffnet sich der Übersichtsbildschirm. Wählen Sie auf der Grundlage der Erläuterungen in Abschnitt 6.3.2 die Betriebsart des Geräts aus und klicken Sie auf „Save Settings [Einstellungen speichern]", um zum nächsten Schritt zu gelangen.





Seite zur Einstellung der Betriebsart des Geräts

7.3. Konfiguration des drahtlosen Netzwerks

Die Konfiguration des drahtlosen Netzwerks beinhaltet die nachstehenden Wi-Fi-Grundeinstellungen und die Einstellungen für die Wireless Security.

7.3.1. Wireless-Grundeinstellungen

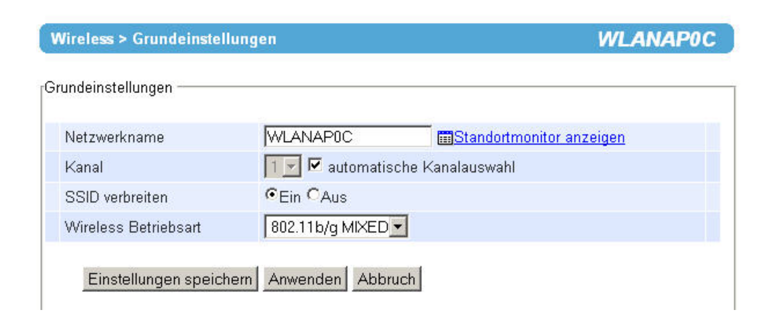
Zur Einrichtung eines Wireless-Netzes werden mehrere Parameter benötigt. Geben Sie den SSID bzw. den Netzwerknamen Ihres Netzes sowie die Kanalnummer Ihres Access Point ein. Der SSID und die Kanalnummer sollten eindeutig sein, um eine Leistungsminderung durch Funkstörungen und SSID-Konflikte zu vermeiden. Mithilfe von „View site monitor [Site Monitor anzeigen]" können Sie SSID und Kanalnummern der umliegenden Access Points in dem Versorgungsbereich des Geräts in Erfahrung bringen. Wenn Sie „Automatic Channel Select [Automatische Kanalwahl]" auswählen, weist das Gerät automatisch die beste verfügbare Kanalnummer zu.

Die Funktion „SSID Broadcast" ermöglicht es Wireless Clients, nach der Anwesenheit dieses Access Point zu suchen. Standardmäßig ist diese Funktion aktiviert. Wenn die Funktion „SSID Broadcast" deaktiviert wird, muss die SSID manuell in die Konfiguration von Wireless Clients eingegeben werden, um die Netzwerksicherheit zu erhöhen und einen Zugriff von unbefugten Clients zu verhindern.

Sie können die „Wireless-Betriebsart" dieses Access Point auch nach Ihrem Bedarf spezifizieren. Standardmäßig ist die Betriebsart 802.11b/g GEMISCHT eingestellt, die in der Regel mit allen Wireless-Clients kompatibel ist.



Wenn Sie die Konfiguration der Wireless Security abgeschlossen haben, klicken Sie auf **„Save Settings** [Einstellungen speichern]**“**, um zum nächsten Schritt zu gelangen.



Grundeinstellungen der Drahtlosverbindung des Access Point

7.3.2. Konfiguration der Wireless Security

Über die Wireless-Security-Einstellungen kann die Netzwerksicherheit an die Erfordernisse des Benutzers angepasst werden. Standardmäßig ist die Wireless-Security deaktiviert. Der Standard-Authentifizierungsmodus ist offen und ohne Verschlüsselung.

Es werden drei Sicherheitsstandards unterstützt: WEP, WPA, und WPA2. Die Client-Authentifizierung erfolgt in WPA und WPA2 entweder über einen vorher vereinbarten Schlüssel "Pre-Shared-Key" (PSK) oder über einen RADIUS-Server.

Es wird empfohlen, WPA2 in Verbindung mit dem PSK-Verfahren zu verwenden. Wählen Sie dazu als Authentifizierungsmodus WPA2-PSK und als Verschlüsselungsart AES aus. Geben Sie das Passwort in die Felder "Passphrase" und "Passphrase bestätigen" ein. In den Wireless-Konfigurationen der Wireless-Clients muss die gleiche Passphrase eingegeben werden, damit die Zugangsbewilligung erteilt wird.

Nachstehend ist die empfohlene Sicherheitskonfiguration angegeben.

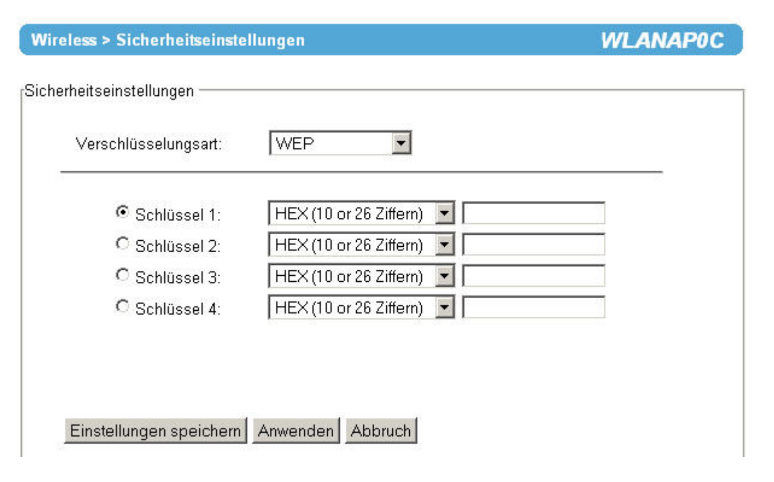
Sicherheitsart	Authentifizierungsmodus	Verschlüsselungsart	Passwort
Deaktiviert	OFFEN	KEINE	Nicht zutreffend
WEP	OFFEN	WEP	Passworteingabe in WEP-Tabelle. Es sind vier Einträge möglich. Wenn Sie in den jeweiligen Wireless-



			Konfigurationen der Wireless-Clients den entsprechenden Key Index angeben, können die Wireless Clients alle vier Passwörter verwenden. Der ausgewählte Key Index wird standardmäßig verwendet, wenn der WLANAP0C mit den Wireless Clients kommuniziert.
WPA-PSK	WPA-PSK	TKIP	Passwort in Passphrase-Feld
WPA2-PSK	WPA2-PSK	AES	Passwort in Passphrase-Feld

Erweiterte Einstellungen für die Wireless-Security unter Verwendung von RADIUS-Servern finden sich in der Konfiguration der "Web Console".

Wenn Sie die Konfiguration der Wireless Security abgeschlossen haben, klicken Sie auf **„Save Settings** [Einstellungen speichern]**"**, um zum nächsten Schritt zu gelangen.



Wireless-Security-Einstellungen für WEP-Key



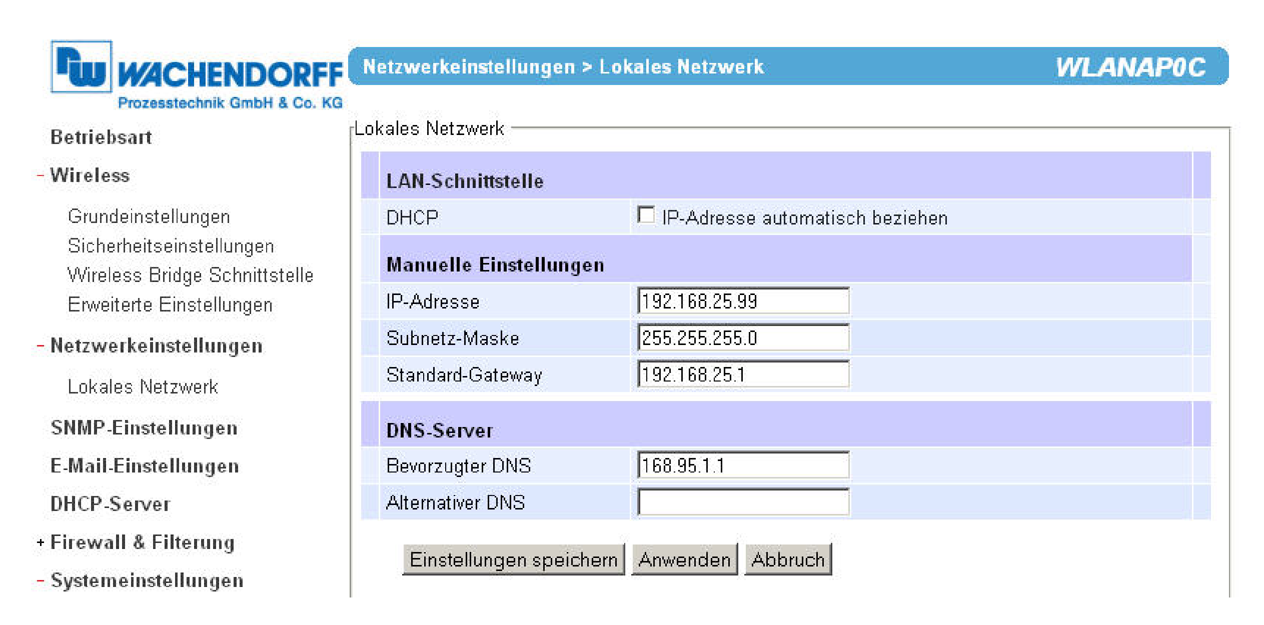
7.4. Konfiguration der Netzwerk-Adresse

Die Adresseinstellungen sind für jede Betriebsart des Geräts leicht unterschiedlich. Befolgen Sie je nach der Betriebsart des Geräts die folgenden Anweisungen.

7.4.1. Einstellungen der Netzwerkadresse für den Betrieb als Access Point

Unten ist der Screenshot für die Einstellungen der Netzwerkadresse im normalen Access-Point-Betrieb dargestellt. Die IP-Adresse des Geräts kann entweder automatisch vom DHCP-Server bezogen werden oder sie kann manuell eingestellt werden. Zur manuellen Einstellung der IP-Adresse des Geräts werden eine zuvor zugewiesene IP-Adresse, die Subnetzmaske und der Standard-Gateway des LAN benötigt. Wenden Sie sich bitte an Ihren Netzwerkadministrator, wenn Ihnen diese vordefinierten Werte nicht vorliegen.

Die IP-Adresse des DNS-Servers wird nur benötigt, wenn Sie die Wireless Clients an das Internet anschließen. Die IP-Adresse Ihres DNS-Servers können Sie bei Ihrem Administrator in Erfahrung bringen.



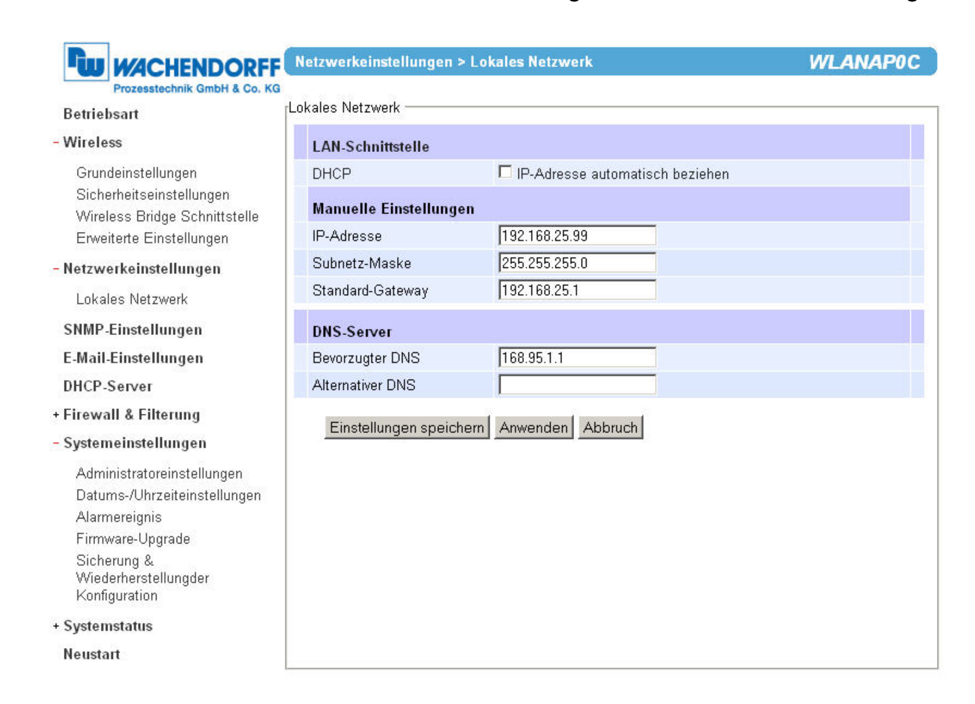
Netzwerk-Einstellung auf der LAN- und der WLAN-Schnittstelle für den Access-Point-Betrieb

7.4.2. Einstellungen der Netzwerkadresse für den Betrieb als Wireless Bridge

Im Wireless-Bridge-Betrieb können Sie eine IP-Adresse über das DHCP automatisch beziehen. Andernfalls können Sie IP-Adresse, Subnetzmaske und Standard-Gateway des Geräts auch manuell



angeben. Wenn Sie wollen, dass sich die verdrahteten Clients mit dem Internet verbinden können, geben Sie bitte auch die IP-Adresse des DNS-Servers Ihres Netzwerks an. Wenden Sie sich bitte an Ihren Netzwerkadministrator, wenn Ihnen keine vorher zugewiesene IP-Adresse vorliegt.

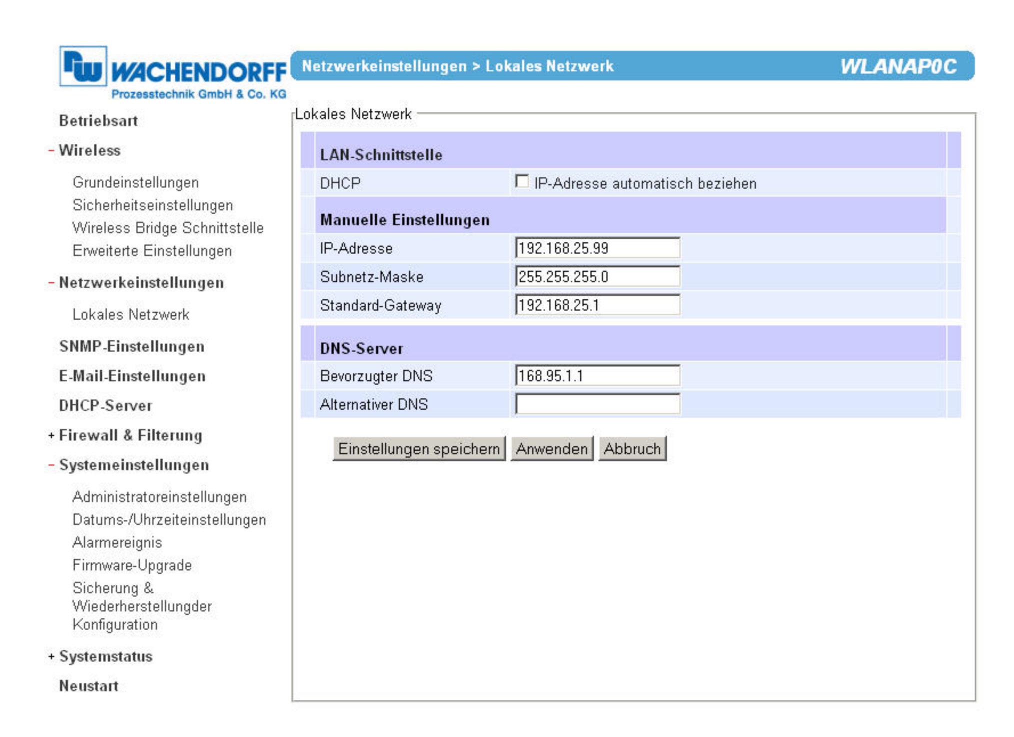


Netzwerkeinstellungen auf der LAN-Schnittstelle für den Betrieb als Wireless Bridge

7.4.3. Einstellungen der Netzwerkadresse für den Betrieb als AP + Wireless Bridge

Die Einstellungen der Netzwerkadresse für den AP + Wireless-Bridge-Betrieb des Geräts sind ähnlich wie die Einstellungen im Wireless-Bridge-Betrieb. Die Adresseneinstellungen für den Wireless-Bridge-





Netzwerkeinstellungen auf der LAN-Schnittstelle für den Betrieb als AP + Wireless Bridge

7.5. Leitfaden zum Konfigurationsablauf

In diesem Abschnitt finden sich Hinweise für den Administrator zur richtigen Einstellung des Geräts auf der Grundlage seiner Betriebsart.

7.5.1. Einstellungen für den AP-Betrieb

Nachstehend ist der Konfigurationsablauf für den Access-Point-Betrieb dargestellt.

Schritt 1: Wählen Sie auf der Übersichtseite [Overview] den AP-Betrieb [Access Point] aus und klicken Sie auf „Einstellungen speichern [Save Settings]"

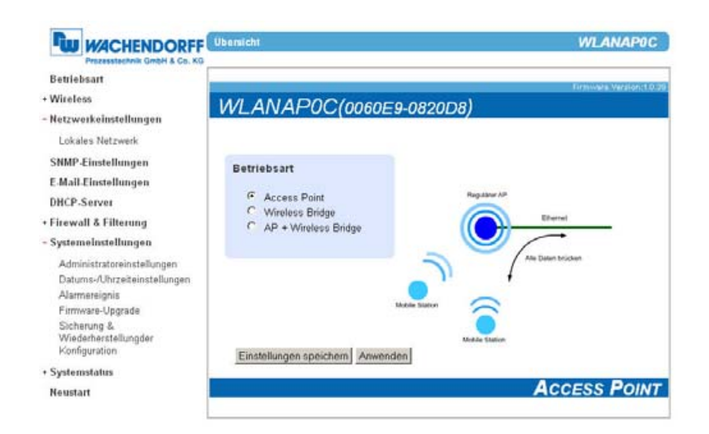
Schritt 2: Ändern Sie auf der Seite „Grundeinstellungen" [Basic Settings] gegebenenfalls die SSID und klicken Sie auf „Einstellungen speichern" [Save Settings].

Schritt 3: Stellen Sie auf der Seite „Sicherheitseinstellungen" [Security Settings] die Sicherheits-funktionen nach Ihren Wünschen ein und klicken Sie auf „Einstellungen speichern" [Save Settings].

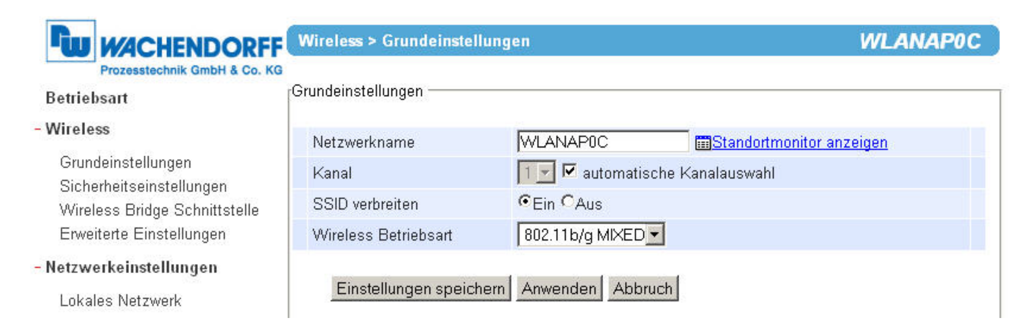
Schritt 4: Geben Sie auf der Seite „LAN- und WLAN-Schnittstelle" [LAN & WLAN Interfaces] entsprechend Ihrer Netzwerk-konfiguration „IP-Adresse" [IP Address], „Subnetzmaske" [Subnet Mask] und „Standard-Gateway" [Default Gateway] ein.

Schritt 5: Klicken Sie auf „Anwenden" [Apply], um die Einstellungen zu speichern und die aktuellen Konfigurationen zu aktivieren.

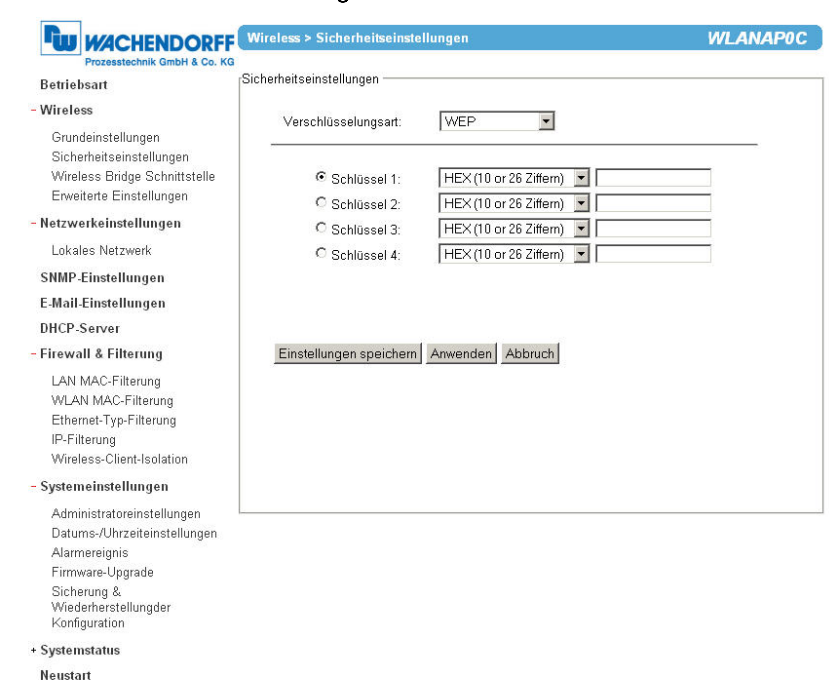




Konfiguration im AP-Betrieb: Schritt 1

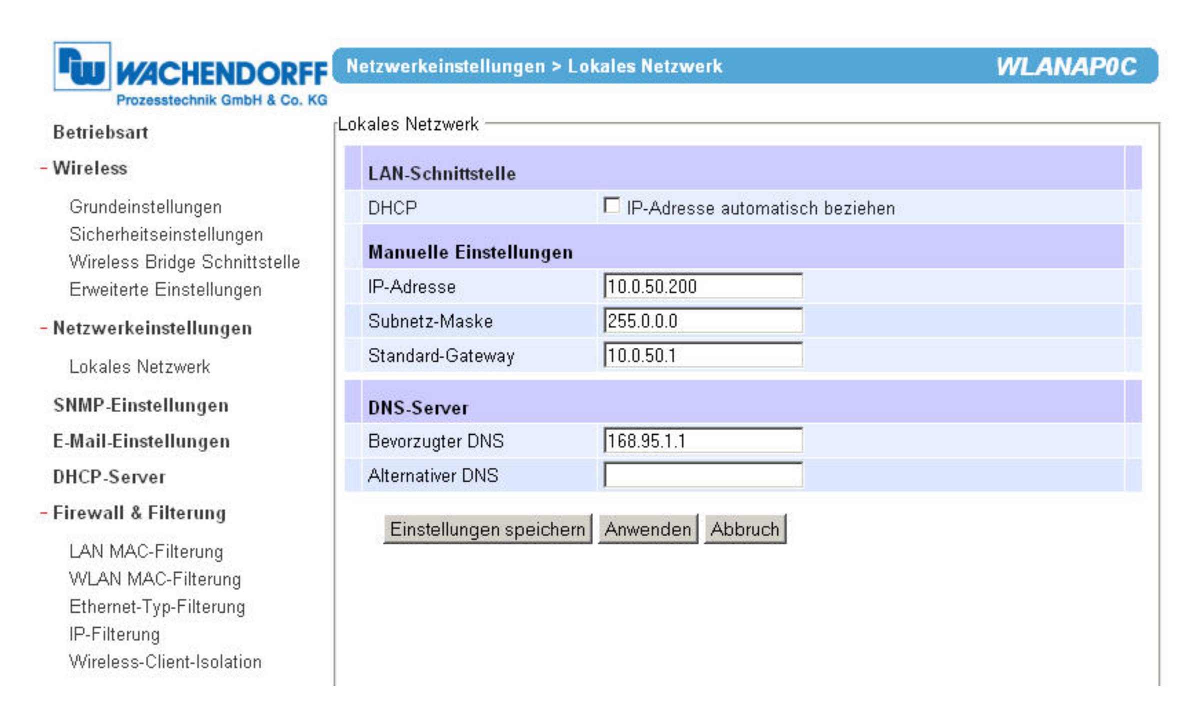


Konfiguration im AP-Betrieb: Schritt 2



Konfiguration im AP-Betrieb: Schritt 3





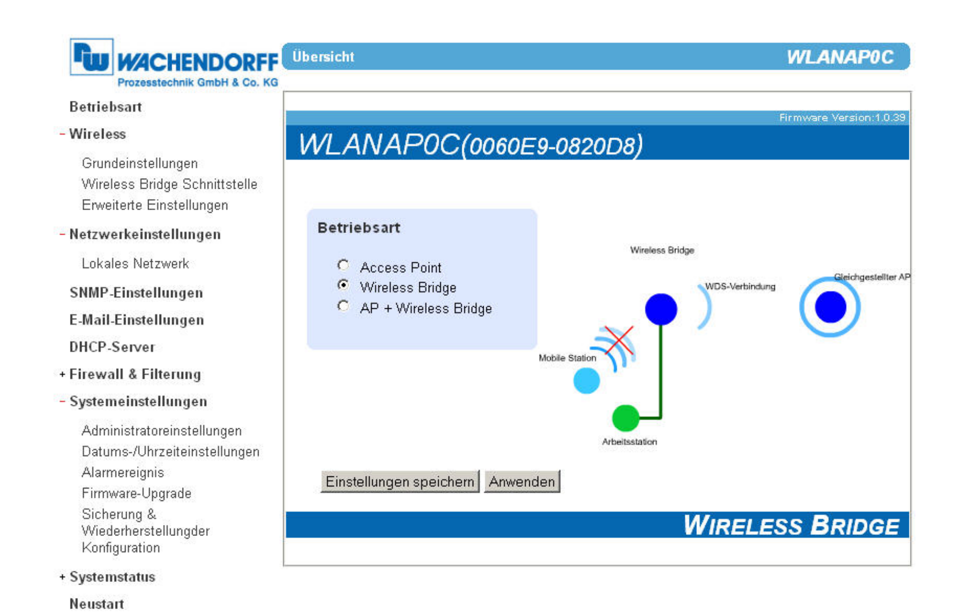
Konfiguration im AP-Betrieb: Schritt 4 und 5



7.5.2. Konfiguration im Wireless-Bridge-Betrieb

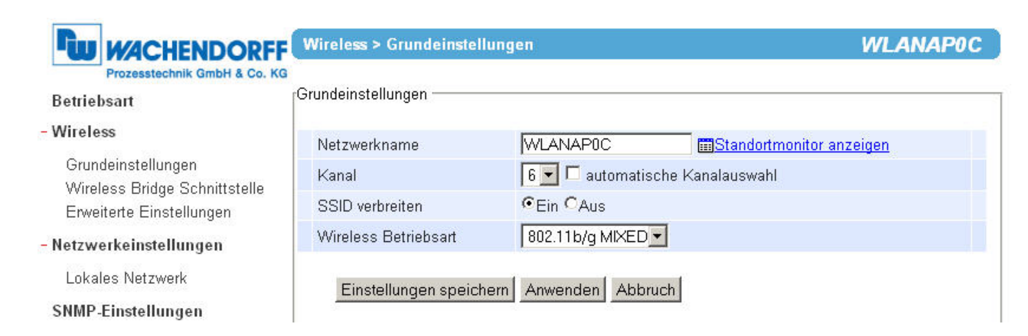
Nachstehend ist der Konfigurationsablauf für den Wireless-Bridge-Betrieb dargestellt.

Schritt 1	Schritt 2	Schritt 3	Schritt 4	Schritt 5
Schritt 1: Wählen Sie auf der Seite „Übersicht“ [Overview] die Betriebsart „AP + Wireless Bridge“ aus und klicken Sie auf „Einstellungen speichern“ [Save Settings].	**Schritt 2**: Ändern Sie auf der Seite „Grund-einstellungen“ [Basic Settings] die SSID, stellen Sie den gewünschten Funkkanal ein und klicken Sie auf „Einstellungen speichern“ [Save Settings].	**Schritt 3**: Stellen Sie auf der Seite „Wireless Bridge-Schnittstelle [Wireless Bridge Interface]“ die gewünschte Sicherheit ein, geben Sie die MAC-Adresse der anderen WLANAP0C-Geräte ein und klicken Sie auf „Einstellungen speichern [Save Settings]“.	**Schritt 4**: Geben Sie auf der Seite „Local Area Networks“ die „IP-Adresse“ [IP Address] die „Subnetzmaske“ [Subnet Mask] und den „Standard-Gateway“ [Default Gateway] ein.	**Schritt 5**: Klicken Sie auf „Anwenden“ [Apply], um die Einstellungen zu speichern und die aktuellen Kon-figurationen zu aktivieren.

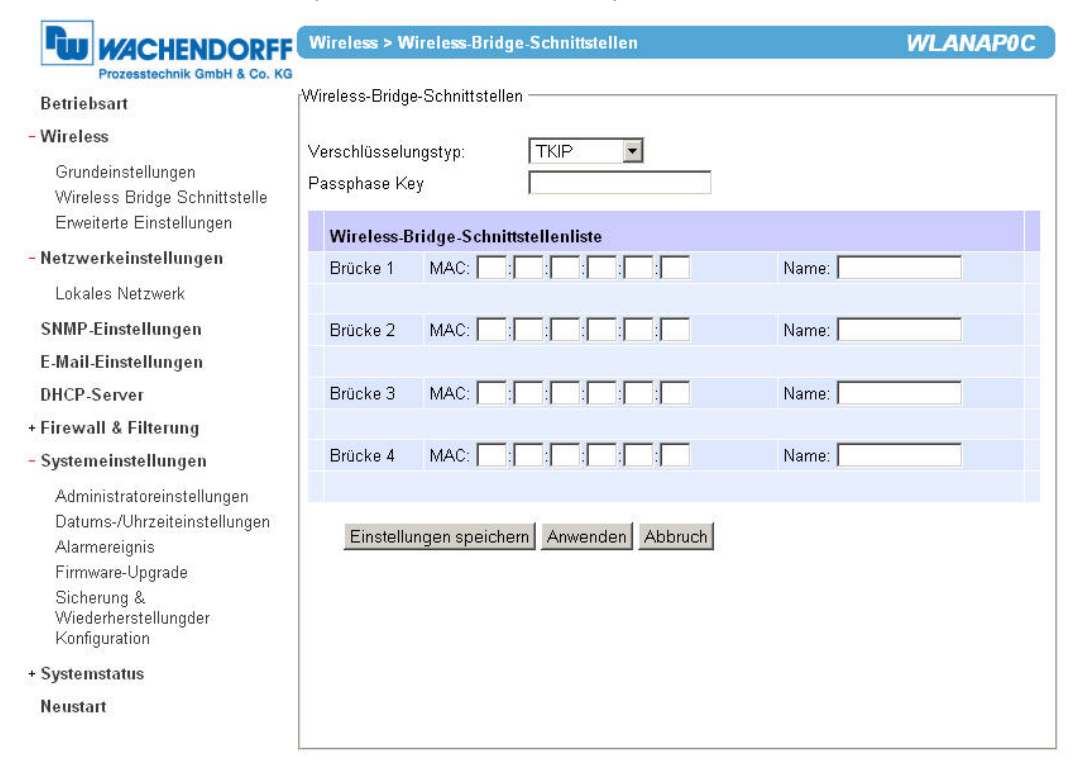


Konfiguration im Wireless-Bridge-Betrieb: Schritt 1



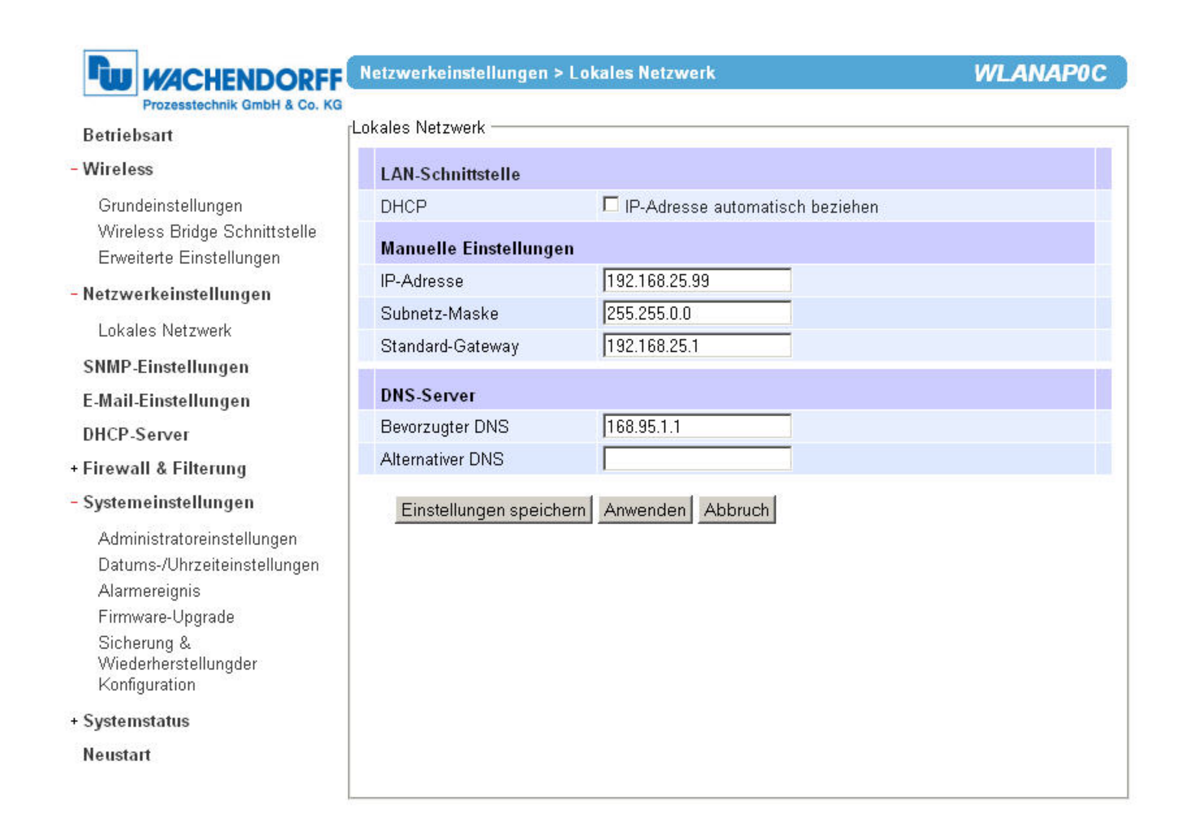


Konfiguration im Wireless-Bridge-Betrieb: Schritt 2



Konfiguration im Wireless-Bridge-Betrieb: Schritt 3





Konfiguration im Wireless-Bridge-Betrieb: Schritt 4 und 5

7.5.3. Konfiguration im „AP + Wireless-Bridge“-Betrieb

Nachstehend ist der Konfigurationsablauf für den „AP + Wireless-Bridge“-Betrieb dargestellt.



Schritt 1: Wählen Sie auf der Seite „Übersicht“ [Overview] die Betriebsart „AP + Wireless Bridge“ aus und klicken Sie auf „Einstellungen speichern“ [Save Settings].

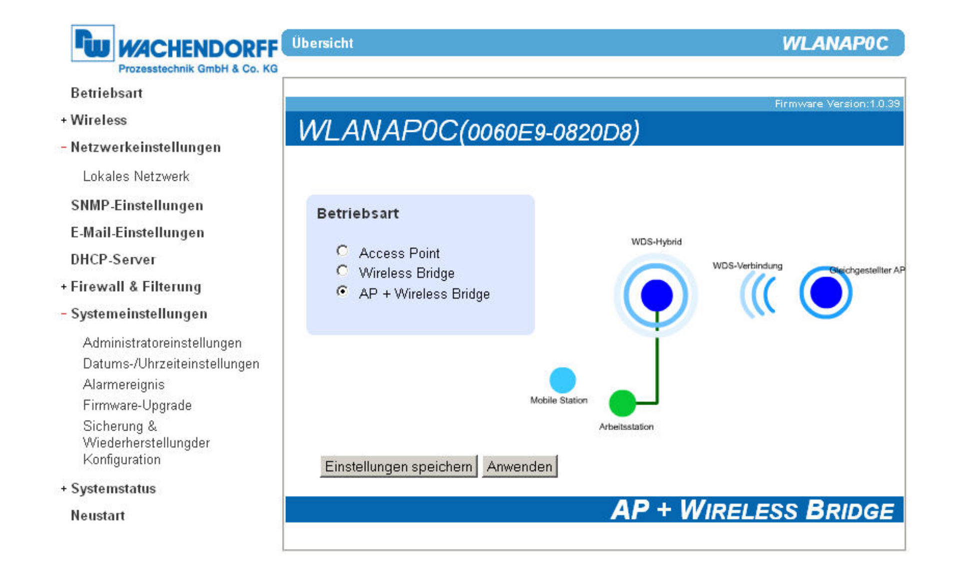
Schritt 2: Ändern Sie auf der Seite „Grundeinstellungen“ [Basic Settings] gegebenenfalls die SSID und klicken Sie auf „Einstellungen speichern“ [Save Settings].

Schritt 3: Stellen Sie auf der Seite „Sicherheits-einstellungen“ [Security Settings] die Sicherheits-funktionen nach Ihren Wünschen ein und klicken Sie auf „Einstellungen speichern“ [Save Settings].

Schritt 4: Stellen Sie auf der Seite „Wireless Bridge-Schnittstelle [Wireless Bridge Interface]“ die gewünschte Sicherheit ein, geben Sie die MAC-Adresse der anderen WLANAP0C-Geräte ein und klicken Sie auf „Einstellungen speichern [Save Settings]“.

Schritt 5: Geben Sie auf der Seite „Local Area Networks“ die „IP-Adresse“ [IP Address] die „Subnetzmaske“ [Subnet Mask] und den „Standard-Gateway“ [Default Gateway] ein.

Schritt 6: Klicken Sie auf „Anwenden“ [Apply], um die Einstellungen zu speichern und die aktuellen Konfigurationen zu aktivieren.

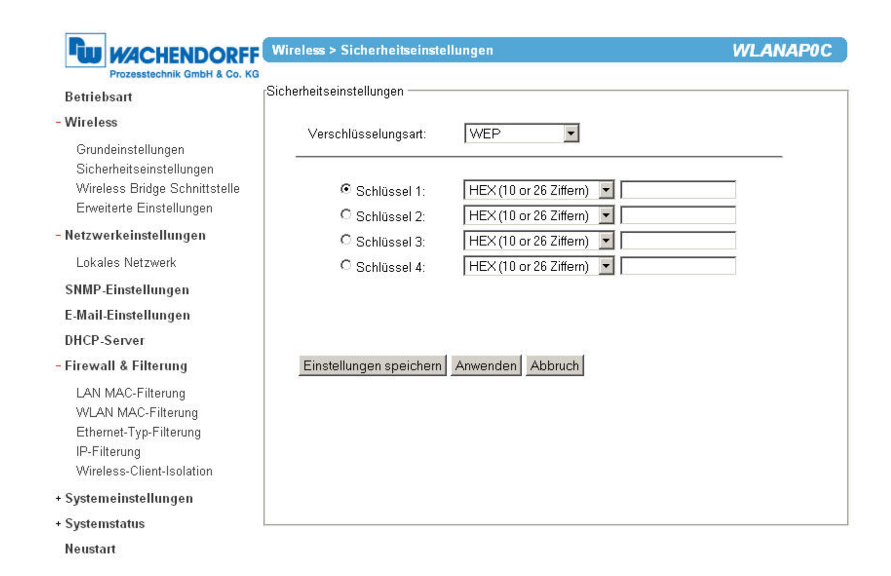


Konfiguration im „AP + Wireless-Bridge“-Betrieb: Schritt 1

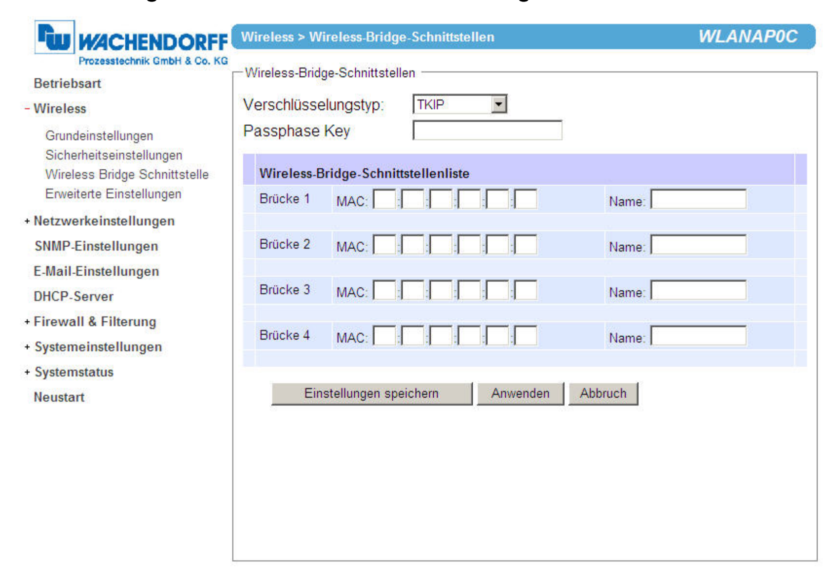


Konfiguration im „AP + Wireless-Bridge“-Betrieb: Schritt 2

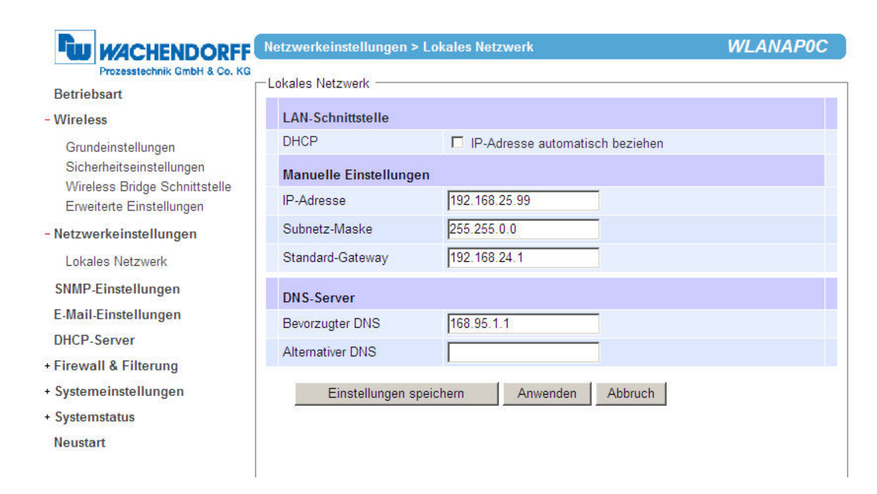




Konfiguration im „AP + Wireless-Bridge“-Betrieb: Schritt 3



Konfiguration im „AP + Wireless-Bridge“-Betrieb: Schritt 4

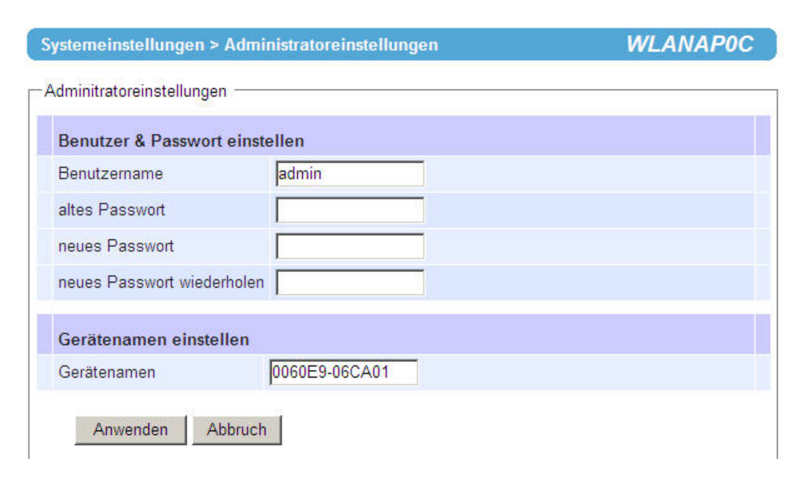




Konfiguration im „AP + Wireless-Bridge“-Betrieb: Schritt 5 und 6

7.6. Administrator-Passwort und Benutzer-Passwort ändern

Wenn Sie die angeführten Einstellungen im vorhergehenden Kapitel abgeschlossen haben, empfehlen wir, das Administrator-Passwort (admin) zu ändern, um einen unbefugten Zugriff auf Ihren Access-Point zu verhindern. Der Screenshot der Einstellungen für die Benutzer- und Passworteinstellungen ist dargestellt in der unteren Abbildung. Geben Sie zum Ändern des Administrator-Passworts unter „Benutzername“ [User name] „admin“ und unter „Altes Passwort“ [Old password] das Standardpasswort ein. Geben Sie Ihr neues Administrator-Passwort als „Neues Passwort“ [New password] ein und wiederholen Sie es erneut unter „Neues Passwort wiederholen“ [Repeat new password]. Klicken Sie auf „Anwenden“ [Apply], um Ihr neues Passwort zu speichern.

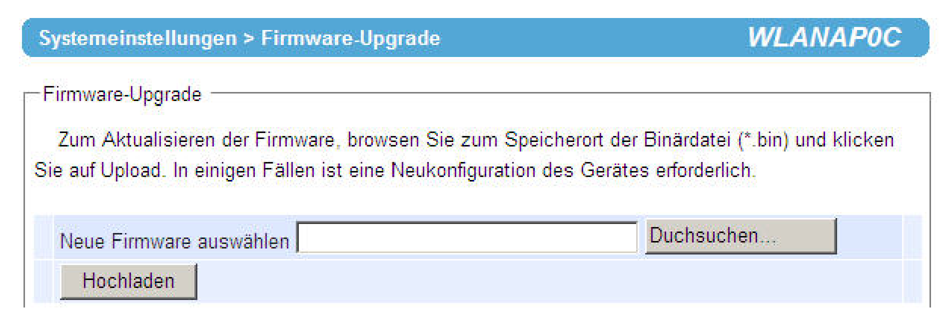


Benutzer- und Passworteinstellungen

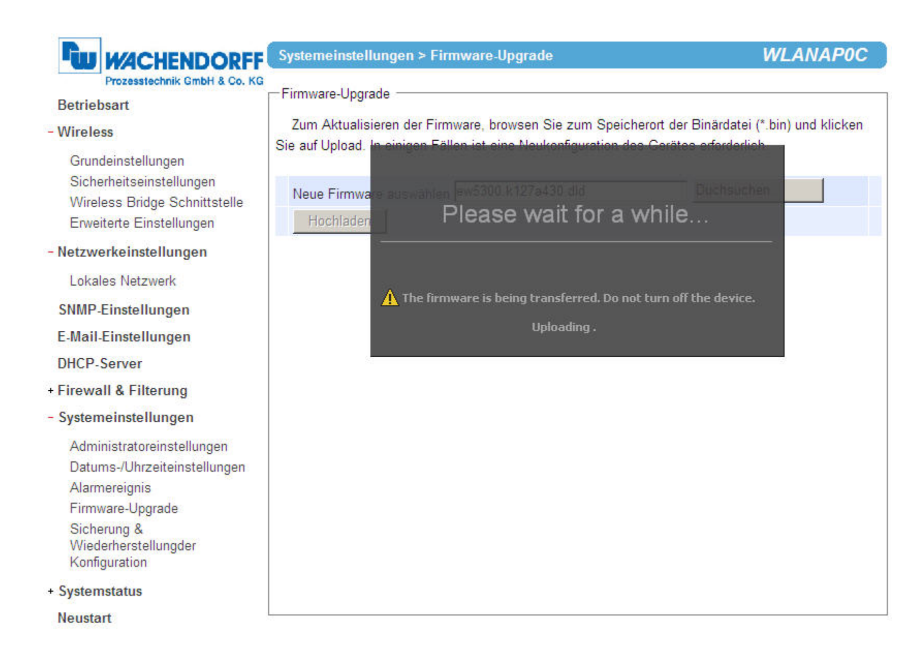
7.7. Firmware aktualisieren

Gelegentlich müssen Sie die Firmware Ihres Access-Point aktualisieren, um Fehlerbehebungen oder neue Funktionen zu integrieren. Gehen Sie zur Aktualisierung der Firmware zum Menü „Systemkonfiguration“ [System Setup] und wählen Sie „Firmware aktualisieren“ [Firmware Upgrade]. Klicken Sie auf „Durchsuchen“ [Browse], um zum Downloadbereich Ihrer neuen Firmware zu gelangen. Stellen Sie bitte sicher, dass das Gerät über eine zuverlässige Stromversorgung verfügt und dass es während der Firmware-Aktualisierung nicht neu gestartet wird, bevor Sie auf die Schaltfläche „Hochladen“ [Upload] klicken. Klicken Sie anschließend auf „Hochladen“ [Upload], um die neue Firmware zu aktualisieren. Führen Sie während der Aktualisierung bitte keinen Neustart des Geräts durch und schalten Sie die Stromversorgung nicht ab. Nach Abschluss der Aktualisierung wird das Gerät automatisch neu gestartet. Die Firmware-Aktualisierung dauert etwa 1 Minute. Einige Parameter müssen Sie nach der Firmware-Aktualisierung unter Umständen neu einstellen.





Firmware-Aktualisierung in der Systemkonfiguration

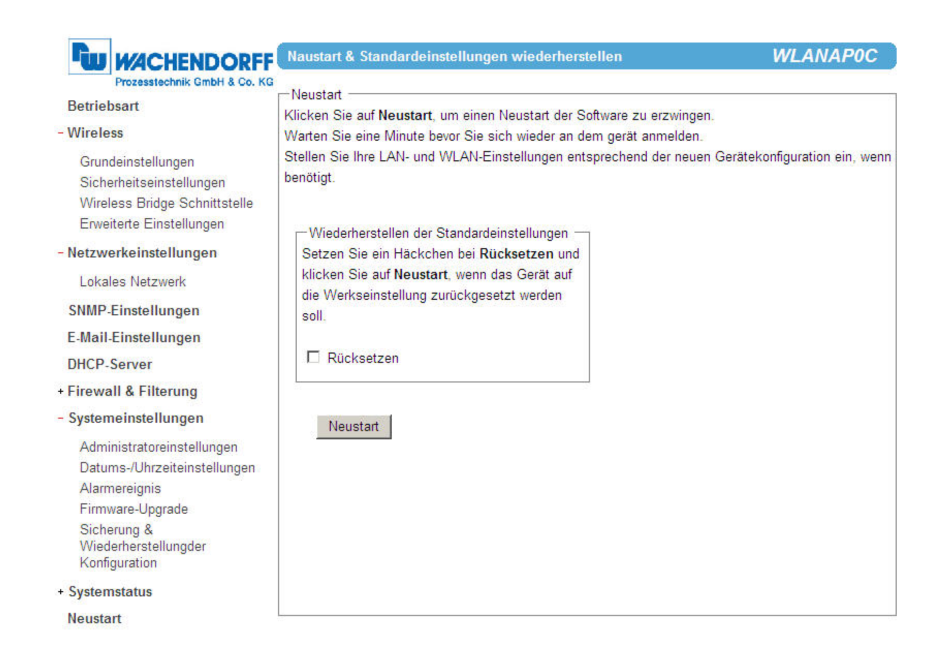


Firmware-Aktualisierung läuft gerade. Schalten Sie das Gerät bitte nicht aus.

7.8. Werkseinstellungen wiederherstellen

Unter Umständen kann es vorkommen, dass Sie das Gerät auf die Werkseinstellungen zurückstellen wollen, beispielsweise wenn Sie das Administrator-Passwort vergessen haben oder einige Parameter falsch eingestellt haben. Kreuzen Sie dazu das Kästchen „Reset“ an und klicken Sie auf „Neu starten“ [Reboot], um Ihr Gerät mit den Werkseinstellungen neu zu starten.





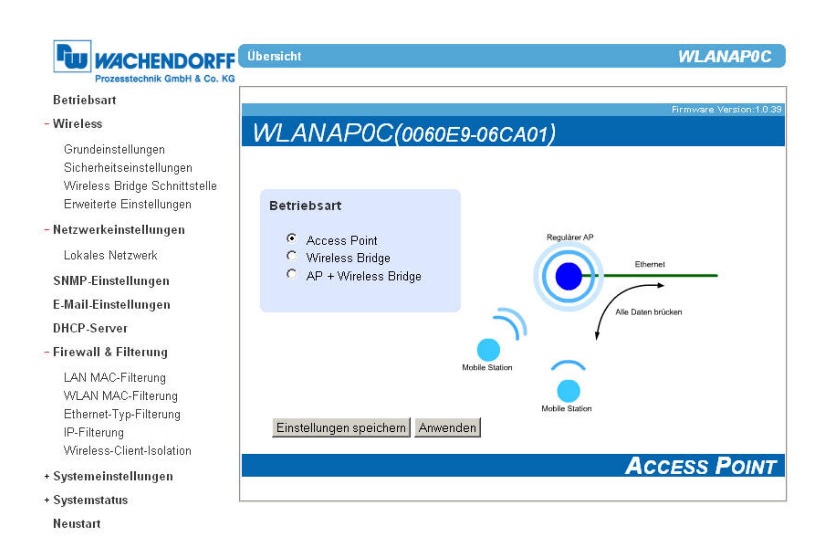
Gerät neu starten bzw. Gerät auf die Werkseinstellungen zurückstellen

8. Konfiguration der Webkonsole

In diesem Kapitel erklären wir in den folgenden Abschnitten die Konfiguration des Wireless Access Point WLANAP0C für alle Funktionalitäten, die einen Webbrowser verwenden.

8.1. Übersichtsinformationen

Sobald Benutzername und Passwort korrekt eingegeben wurden, wird die Webseite „Übersicht“ [Overview] folgendermaßen angezeigt. Das Menü „Einstellungen“ [Settings] befindet sich in der linken Spalte. Die Webseite „Übersicht“ [Overview] des Geräts ist je nach den einzelnen Betriebsarten des Geräts leicht unterschiedlich.





8.2. Wireless-Einstellungen

Unter den Wireless-Einstellungen finden sich die „Grundeinstellungen“ [basic settings], die „Sicherheitseinstellungen“ [Security settings], die „Erweiterten Einstellungen“ [Advanced settings] sowie spezielle Einstellungen, wie zum Beispiel die Einstellungen für die Wireless-Bridge-Schnittstelle.

8.2.1. Grundeinstellungen [Basic Settings]

Die Grundeinstellungen umfassen die Konfiguration der Grundfunktionen des drahtlosen Netzwerks.

Netzwerkname (SSID)

Die SSID wird zur Identifizierung des drahtlosen Netzwerks des Geräts verwendet. Sie kann aus einem alphanumerischen Wort ohne Leerzeichen bestehen. Im normalen Access-Point-Betrieb muss sie in Ihrer Netzwerkumgebung eindeutig sein. Klicken Sie auf „Site Monitor anzeigen“ [View site monitor], um andere drahtlose Netzwerke in Ihrem Gebiet zu prüfen. In den Betriebsarten „Wireless Bridge“ und „WDS Hybrid“ muss die SSID dieselbe sein wie die SSID der anderen drahtlosen Netze. Über die Schaltfläche „Site Monitor anzeigen“ [View site monitor] können Sie die SSID der anderen Netze einsehen.

Kanal

Der Kanal wird von dem Gerät zur Datenübertragung über eine drahtlose Verbindung verwendet. Im Access-Point-Betrieb muss sie in einer drahtlosen Umgebung eindeutig sein. Es wird empfohlen, nicht überlappende Kanäle zu verwenden, also Kanalnummer 1, 6 und 11. Wenn Sie auf „Site Monitor anzeigen“ [View site monitor] klicken, können Sie die von anderen Netzwerken verwendeten Kanäle einsehen. Wenn Sie „Automatische Kanalauswahl“ [Automatic Channel Select] auswählen, wählt das Gerät den Kanal automatisch aus. In der Betriebsart „Wireless Bridge“ muss der von dem Gerät verwendete Kanal derselbe sein wie der von dem anderen Netzwerk verwendete Kanal.

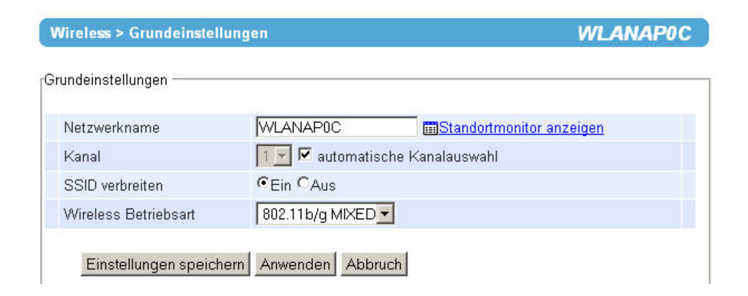
SSID-Broadcast

Standardmäßig ist der SSID-Broadcast aktiviert, damit Mobilstationen das Gerät suchen und sich automatisch mit ihm verbinden können. Allerdings ist das Gerät dadurch der Gefahr eines unbefugten Zugriffs ausgesetzt, wenn keine Wireless-Security-Einstellungen vorgenommen werden (Informationen zur Einstellung der Wireless-Security finden Sie unter „Sicherheitseinstellungen“ [Security Settings]). Sie können den SSID-Broadcast auch deaktivieren. Wenn der „SSID-Broadcast“ deaktiviert wird, müssen Sie die SSID manuell in eine Mobilstation eingeben, um sie mit diesem Gerät zu verbinden.

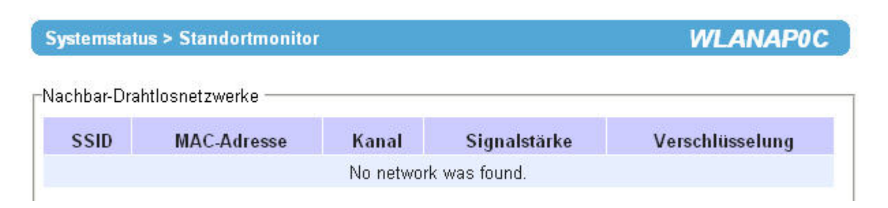
Wireless-Modus



Das Gerät kann in verschiedenen Wireless-Betriebsarten nach den Standards nur IEEE 802.11b, nur IEEE 802.11g oder 802.11 b/g gemischt [Mixed] betrieben werden. In der Betriebsart IEEE 802.11b/g gemischt [Mixed] unterstützt das Gerät sowohl Mobilstationen mit dem Standard IEEE 802.11b als auch Mobilstationen mit dem Standard 802.11g. In der Betriebsart IEEE 802.11b unterstützt das Gerät Datenraten bis zu 11 Mb/b. In der Betriebsart IEEE 802.11g unterstützt das Gerät Datenraten bis zu 54 Mbps.



Grundeinstellungen der Konfiguration des Wireless-Netzwerks



Snapshots des Site Monitors der umgebenden Netze

8.2.2. Sicherheitseinstellungen

Die Einstellungen der Wireless-Security legen die Sicherheitsmodi des drahtlosen Netzes fest. Es gibt zwei unterschiedliche Sicherheitsfunktionen: Authentifizierung und Verschlüsselung. Es gibt drei verschiedene Authentifizierungsmodi: Open System [Open], Shared Key [Shared] und WPA. Zusätzlich stehen drei verschiedene Verschlüsselungsmethoden zur Verfügung: WEP, TKIP und AES. Die Zusammenfassung der Sicherheitsmodi ist in Tabelle 4-1 dargestellt.

Zusammenfassung der Sicherheitsmodi in den Einstellungen der Wireless Security

	WEP-Modus	WPA-Modus	WPA2-Modus
Authentication Mode	Open	WPA	WPA
Encryption Type	WEP	TKIP	AES



WEP-Modus

Der „Wired Equivalent Privacy (WEP)“-Modus ist der vom Standard IEEE 802.11 ursprünglich bereitgestellte Sicherheitsmodus, der viele bekannte Schwachstellen aufweist. Es wird empfohlen, diesen Modus nicht zu verwenden. Dieser Modus wird allerdings in vielen älteren Wireless Clients unterstützt.

Wenn der Authentifizierungsmodus als „Offen“ [Open] konfiguriert wird, wird eine Mobilstation nicht authentifiziert, wenn sie an das Gerät angeschlossen wird. Wird zur Verschlüsselung von Nachrichten, die zwischen einer Mobilstation und dem Gerät übermittelt werden, WEP verwendet, benötigen das Gerät und die Mobilstation vor der Verbindungsherstellung einen gemeinsamen geheimen Schlüssel. Dieser Schlüssel wird WEP-Schlüssel genannt und wird aus der Schlüsselliste ausgewählt, in der 4 verschiedene Schlüssel zur Verfügung stehen. Der WEP-Schlüssel besteht aus einer Reihe von Hexadezimalzahlen (die Zahlen 0 - 9 und A - F), die entweder 10 oder 26 Ziffern lang ist. Der WEP-Schlüssel kann auch mit einer Zeichenfolge aus 5 oder 13 Zeichen eingestellt werden. Eine längere Zeichenfolge bietet in der Regel eine größere Sicherheit.

Nachstehend werden einige Beispiele für WEP-Schlüssel angeführt. Ein Beispiel für den zehnziffrigen Hexadezimalschlüssel ist „1234567890“ und ein Beispiel für den 26-ziffrigen Schlüssel ist „11223344556677889900ABCDEF“. Ein Beispiel für einen WEP-Schlüssel mit 5 Zeichen wäre „ABCDE“ oder „HALLO“. Ein WEP-Schlüssel mit 13 Zeichen wäre beispielsweise „SCHLUESSELROT“.

In der WEP-Verschlüsselungsart werden alle über die drahtlose Verbindung übertragenen Daten mit dem WEP-Schlüssel mithilfe des RC4-Verschlüsselungsalgorithmus verschlüsselt.

WPA-Modus

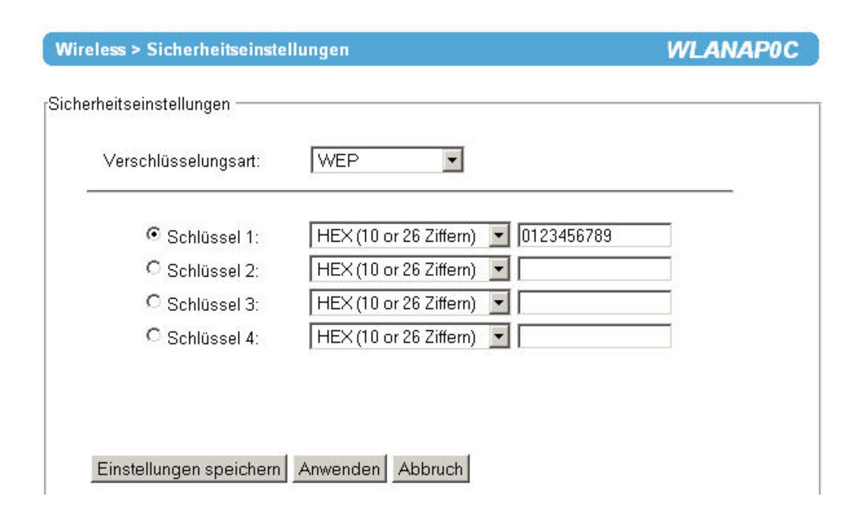
Der „Wi-Fi Protected Access (WPA)“ ist ein neuer Sicherheitsmodus, mit dem die Sicherheitsschwachstellen im WEP-Modus behoben wurden. Der WPA-Modus bietet eine neue Authentifizierungsmethode, die das „Encapsulated Authentication Protocol“ (EAP) und neue Verschlüsselungsarten wie zum Beispiel TKIP und AES nutzt.

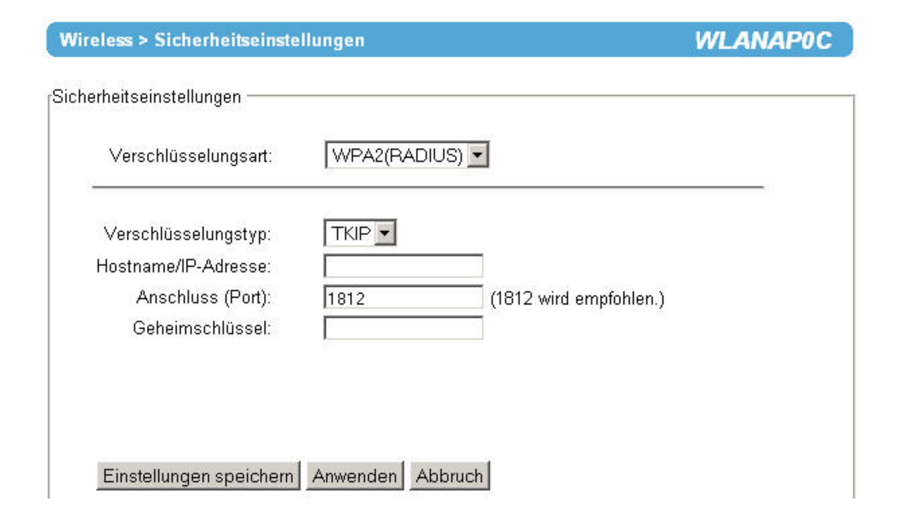
Ein EAP-PSK ist ein EAP-Authentifizierungsmodus mit „Pre-Shared Key“ (PSK). Dieser Modus wird manchmal auch WPA-Personal genannt. In der Regel wird er für Heim- oder Büronetzwerke verwendet, die über keinen RADIUS-Server verfügen. Zur Nutzung dieses Modus müssen Sie eine Passphrase einrichten. Eine Passphrase ist eine Reihe von Worten, die länger sind als ein Passwort. Es kann sich dabei um ein Satzglied oder um einen Satz handeln. Ein Beispiel für eine Passphrase lautet „Dies ist Ihr neues Drahtlosnetzwerk“. Die Passphrase wird auch beim Einrichten eines Anschlusses für eine Mobilstation verwendet. Die Passphrase ist maximal 64 Zeichen lang.

Ein EAP-TTLS oder PEAP ist der üblicherweise verwendete EAP-Authentifizierungsmodus mit einem RADIUS-Server. Dieser Modus wird manchmal auch WPA-Enterprise genannt. Zur Nutzung dieses

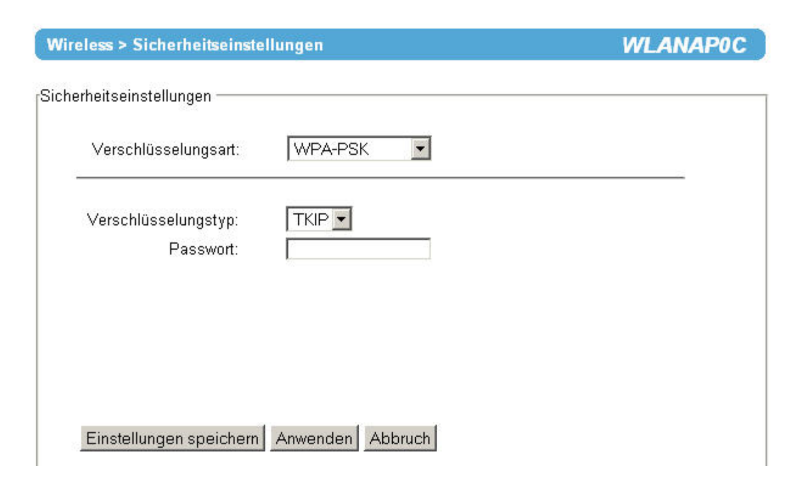


Modus wird die IP-Adresse eines RADIUS-Servers benötigt. Der von dem RADIUS-Server verwendete UDP-Port ist standardmäßig auf Port 1812 gemäß RFC2138-Standard eingestellt. Schließlich muss das Shared Secret, das im RADIUS-Server eingerichtet wurde, dem Gerät ermöglichen, mit dem RADIUS-Server zu kommunizieren. Die IP-Adresse, den RADIUS-Port und das Shared Secret des RADIUS-Servers in Ihrem Netzwerk können Sie bei Ihrem Netzwerk-Administrator in Erfahrung bringen.





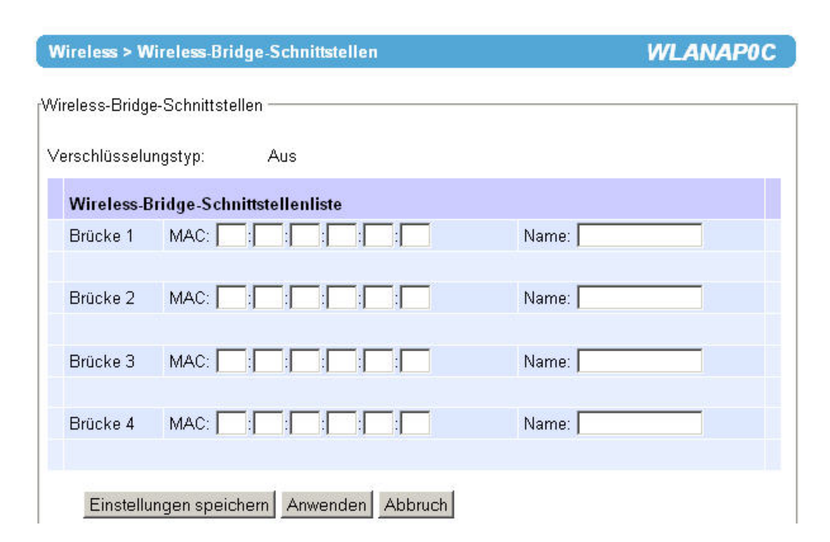




Wireless-Security-Einstellungen

8.2.3. Wireless-Bridge-Schnittstelle

Der WLANAP0C bietet die Möglichkeit, sowohl kabelgebundene als auch drahtlose lokale Geräte mit einem anderen Drahtlosnetzwerk zu verbinden. Das Gerät kann bis zu 4 andere WLANAP0C-Geräte verbinden, indem ihre MAC-Adressen in der Konfiguration eingegeben werden. Die Sicherheit der Verbindung wird nach den vorhergehenden erläuterten Sicherheitsstandards bereitgestellt.

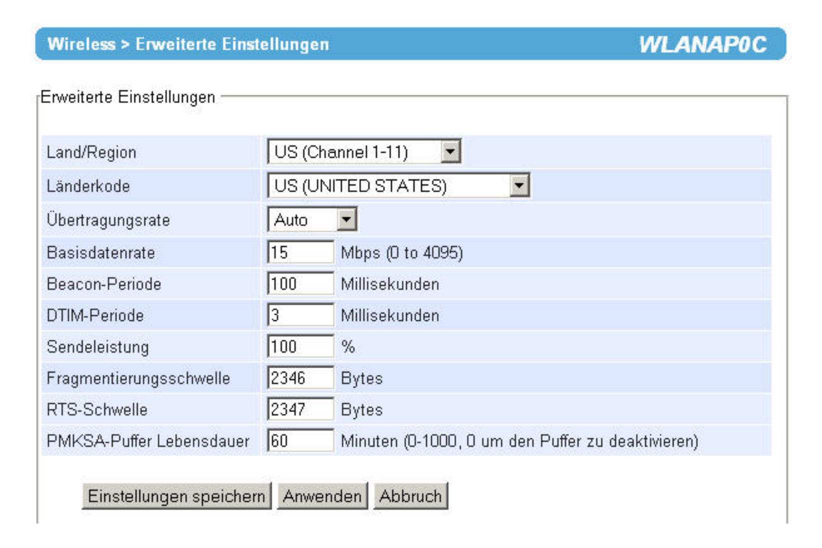


Wireless-Bridge-Schnittstelle

8.2.4. Erweiterte Einstellungen

Die Erweiterten Einstellungen des Geräts liefern die einzelnen Parameter des drahtlosen Netzwerks zur Feineinstellung der Netzwerkleistung. In den meisten Fällen müssen Sie die Parameter nicht verändern. Sie können zur Einhaltung der Bestimmungen Ihres Landes lediglich „Land Region“ [Country Region] und „Landescode“ [Country Code] ändern. Änderungen der anderen Parameter wirken sich auf die Leistung des Netzwerks aus. Gehen Sie beim Ändern der Parameter deshalb bitte umsichtig vor.





Wireless-Einstellungen der Erweiterten Wireless-Parametern

8.3. Netzwerkeinstellungen

8.3.1. LAN-Schnittstelle

LAN-Schnittstelle

Das Gerät kann von dem DHCP-Server, der an die LAN-Schnittstelle angeschlossen ist, eine IP-Adresse beziehen. Wenn Sie das Kästchen „IP-Adresse automatisch beziehen" [Obtain an IP Address Automatically] ankreuzen, bezieht das Gerät automatisch eine IP-Adresse.

Manuelle Einstellungen

Wenn das Netzwerk über keinen DHCP-Server verfügt, kann die IP-Adresse für das Gerät auch manuell eingerichtet werden. IP-Adresse und Subnetzmaske sind verbindlich. Die Standard-Gatewayadresse ist dann erforderlich, wenn Sie das Gerät und die dazugehörenden Mobilstationen ans Internet anschließen müssen.

DNS-Server

Zum Anschluss des Geräts und der dazugehörenden Mobilstationen ans Internet ist die DNS-Adresse erforderlich, um die URL und jeden Domainnamen aufzulösen. Der bevorzugte DNS wird als erstes verwendet und wenn dieser nicht funktioniert, wird der alternative DNS verwendet. Die IP-Adressen der DNS-Server werden automatisch zugewiesen, wenn Sie „IP-Adresse automatisch beziehen" [Obtain IP address automatically] (vom DHCP-Server) aktivieren. Andernfalls müssen Sie die DNS-Serveradresse von Ihrem Netzwerkadministrator in Erfahrung bringen.

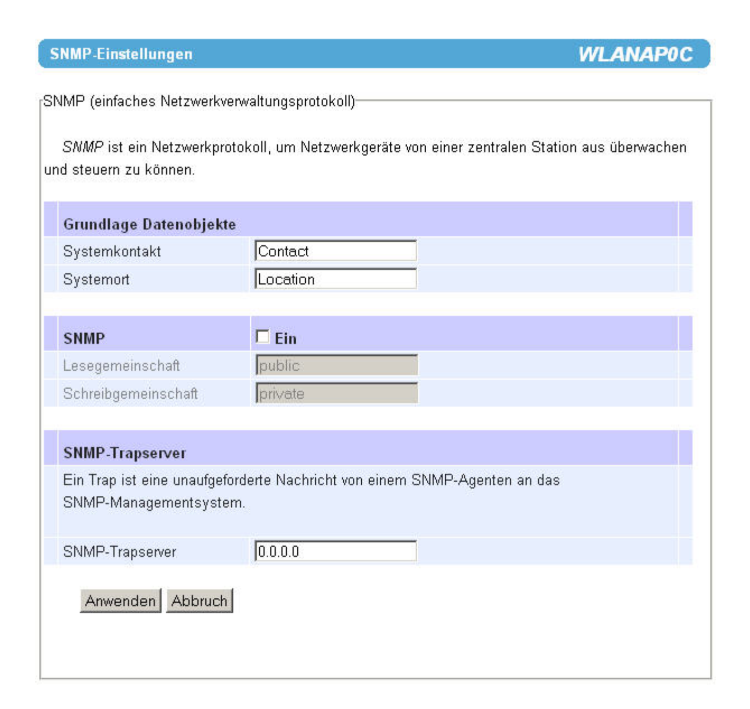


8.4. SNMP-Einstellungen

Das SNMP wird von der Netzwerk-Verwaltungssoftware zur Überwachung von Geräten in einem Netzwerk, zum Auffinden von Informationen zum Netzwerkstatus und zur Konfiguration von Netzwerkparametern verwendet. Die SNMP-Einstellungen zeigen die Konfiguration dieses Geräts, damit es von einer SNMP-Drittsoftware eingesehen werden kann..

Der „System Name“ ist standardmäßig der Gerätename. Der „Systemstandort“ [System Location] ist der Standort des Geräts. Der „Systemansprechpartner“ [System Contact] ist der Name eines Ansprechpartners, in der Regel der Name des Administrators des Geräts.

Wenn Sie die Statusinformationen des Geräts für eine „Read Community“ zugänglich machen wollen, kreuzen Sie ganz einfach das Kästchen SNMP „Enable“ an. Geben Sie in „Read Community“ „public [öffentlich]“ ein. Wenn Sie einer „private [privat]“ genannten Gruppe gestatten wollen, die Parameter des Geräts zu ändern, geben Sie in „Write Community“ „private [privat]“ ein. In einigen Fällen meldet das Gerät einen Alarm aufgrund von Störungen, einer Fangvorrichtung (Trap), einer unbefugten Nachricht, die von einem SNMP-Agenten an den SNMP-Trap-Server geschickt wurde. Geben Sie zum Einrichten eines SNMP-Trap-Servers die IP-Adresse des Trap-Servers ein, der alle Alarmmeldungen sammeln soll. Alle vorgenommenen Änderungen werden nach einem Neustart des Geräts wirksam.



SNMP-Einstellungen

8.5. E-Mail-Einstellungen

In einigen Fällen schickt das Gerät bei Alarmmeldungen eine E-Mail an die Mailbox des Benutzers, um auf den Alarm aufmerksam zu machen. Mit den E-Mail-Einstellungen können Sie das Gerät so



einrichten, dass es eine E-Mail versenden kann. Zur Einrichtung der E-Mail-Versendung müssen Sie eine „Sender“-E-Mail-Adresse eingeben, die dann bei der E-Mail unter „Von“ erscheint. Anschließend geben Sie die „Empfänger“-E-Mail-Adresse ein, an die die E-Mail gesendet wird. Sie können die E-Mail an mehrere Empfänger senden lassen, wenn Sie die einzelnen E-Mail-Adressen durch ein Semikolon (;) trennen. Richten Sie als nächstes den E-Mail-Server ein. Zunächst geben Sie dazu die IP-Adresse eines Mail-Servers in Ihrem lokalen Netzwerk ein. Wenn der Mailserver eine Benutzerauthentifizierung erfordert, müssen Sie „SMTP server authentication required [SMTP-Serverauthentifizierung erforderlich]“ aktivieren und Benutzernamen sowie Passwort eines Benutzers eingeben, um auf den Mailserver zum Versenden der E-Mail zugreifen zu können. Die IP-Adresse, den Benutzernamen und das Passwort für Ihren Mailserver können Sie bei Ihrem Netzwerk-Administrator in Erfahrung bringen.



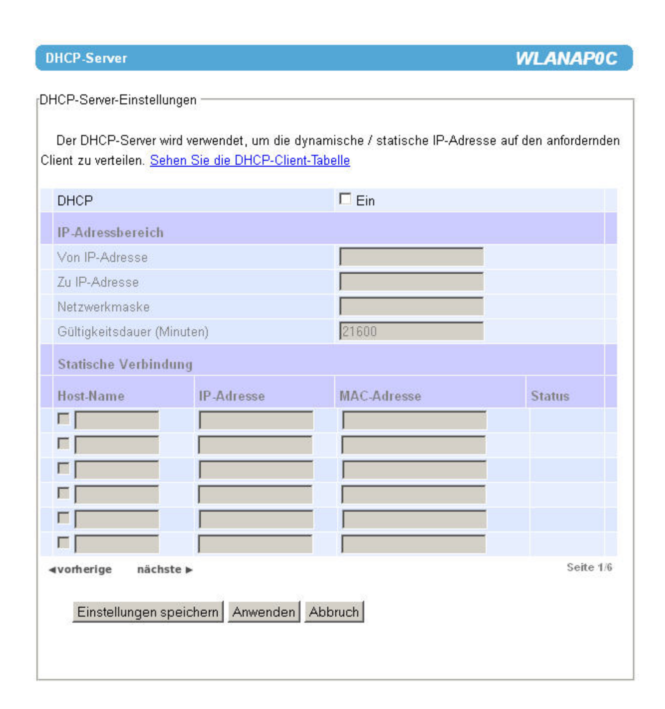
E-Mail-Einstellungen für Alarmmeldungen

8.6. DHCP-Server

In einigen lokalen Netzwerken, wie zum Beispiel in einem SOHO-Netzwerk, gibt es keinen Server, der dem Client als DHCP-Server automatisch eine IP-Adresse zuweisen könnte. Der WLANAP0C kann als DHCP-Server fungieren und mobilen Clients oder Rechnern statisch oder dynamisch eine IP-Adresse zuweisen. Kreuzen Sie zum Aktivieren dieser Funktionalität „DHCP Enabled [DHCP aktiviert]“ an. Anschließend müssen Sie den IP-Adressenbereich einschließlich „Von IP-Adresse [From IP Address]“ und „Zu IP-Adresse [To IP Address]“ eingeben. Geben Sie dann die Subnetzmaske [Subnet Mask] der IP-Adresse ein. Die „Lease Time“ ist die Zeitdauer in Minuten, für die eine einem Gerät zugewiesene IP-Adresse zu diesem Gerät gehört. Ist die Zeit abgelaufen, kann die IP-Adresse einem anderen Gerät zugewiesen werden.



Sie können einem mobilen Client auch eine statische IP-Adresse zuweisen. Eine „statische“ IP-Adresse bedeutet, dass eine solche Adresse niemals abläuft. Sie kann lediglich dem mobilen Client zugewiesen werden. Kreuzen Sie zur statischen Zuweisung einer IP-Adresse das kleine Kästchen vor jeder Zeile an und geben Sie anschließend den „Hostnamen [Host Name]“ die IP-Adresse, die Sie zugewiesen haben wollen und die MAC-Adresse des mobilen Client ein.



Einstellungen des DHCP-Servers

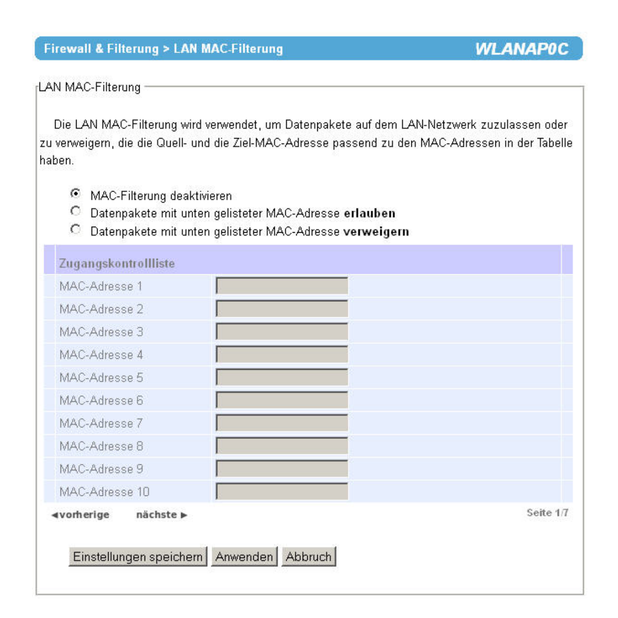
8.7. Firewall und Filterung

In diesem Abschnitt erläutern wir die Firewall- und Paketfilterung-Einstellungen. Datenpakete können auf der Grundlage verschiedener Kriterien gefiltert werden, wie zum Beispiel MAC-Adresse, die Art des Ethernetpakets, IP-Adresse und TCP/UDP-Portnummer. Die Filterungsmethoden bieten eine gewisse Sicherheit vor unbefugten oder bösartigen Datenpaketen und schützen Ihr Gerät und das dazugehörende Netzwerk somit vor einigen Angriffen.

8.7.1. MAC-Filterung (kabelgebunden)

Mit der „Wired MAC Filtering [MAC-Filterung (kabelgebunden)]“ lässt der Filter Pakete durch die kabelgebundene oder LAN/Ethernetschnittstelle passieren oder lehnt sie ab. Wählen Sie zum Aktivieren der kabelgebundenen MAC-Filterung „Only allow MAC Address [nur MAC-Adresse zulassen] oder „Only deny MAC Address [nur MAC-Adresse ablehnen]“ aus und geben Sie die jeweilige MAC-Adressen aller Ethernet-Geräte ein, deren Pakete in der Zugangskontrollliste [Access Control List] zugelassen oder abgelehnt werden sollen.

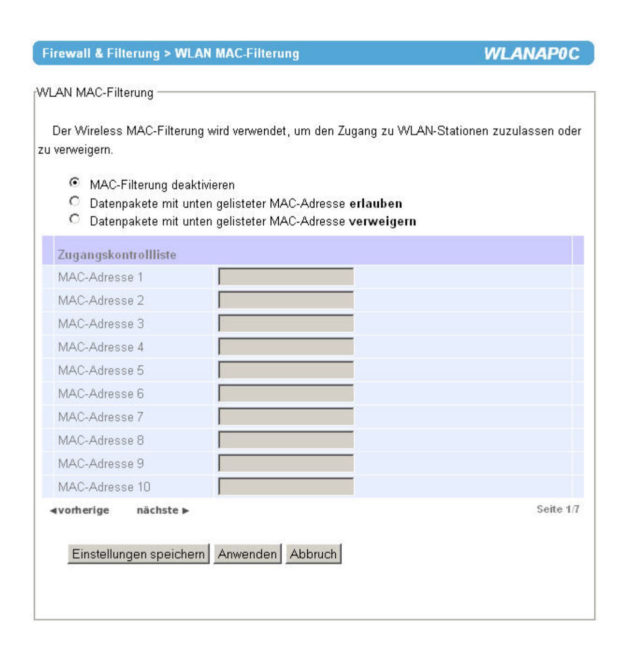




Einstellungen der kabelgebundenen MAC-Filterung

8.7.2. Drahtlose MAC-Filterung (nur für die Betriebsarten „Wireless Bridge“ und „AP + Wireless Bridge“)

Das Gerät bietet auch eine Paketfilterung basierend auf der MAC-Adresse des Wireless-Interface an. Aktivieren Sie „Only allow MAC address [nur MAC-Adresse zulassen]“ oder „Only deny MAC address [nur MAC-Adresse ablehnen]“ zum Einrichten der „Wireless MAC Filtering [Drahtlose MAC-Filterung]“ und geben Sie die MAC-Adressen aller Wireless-Stationen ein, deren Pakete zugelassen bzw. abgelehnt werden sollen.

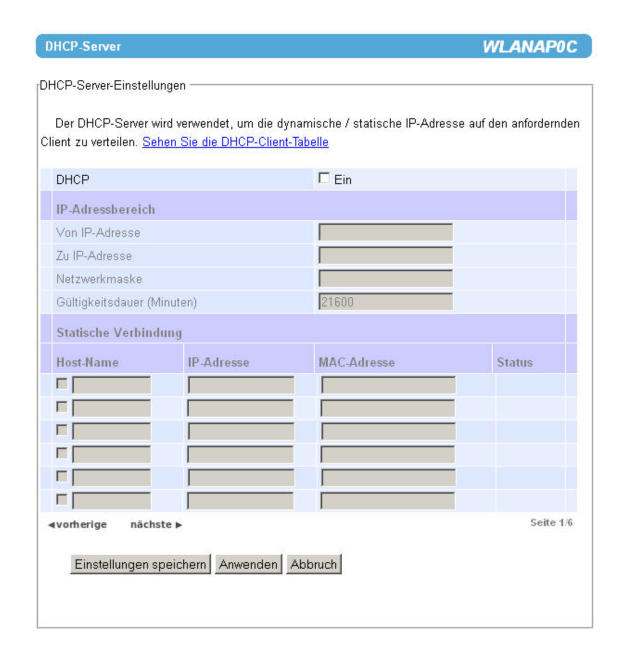


MAC-Filterung (Wireless)



8.7.3. IP-Filterung

Die „IP-Filterung“ aktiviert die Paketfilterung auf der Grundlage des IP-Protokolls, der Quelladresse und der Zieladresse. Wählen Sie zum Hinzufügen eines Filters „Only allow MAC Address [nur MAC-Adresse zulassen]“ oder „Only deny MAC Address [nur MAC-Adresse ablehnen]“ aus. Fügen Sie anschließend den IP-Code des Protokolls, den Protokollnamen, die Quelladresse und die Zieladresse hinzu. Jeder Filter bietet lediglich eine unidirektionale Filterung. Für eine bidirektionale Filterung müssen Sie zwei Filter hinzufügen, von denen jeder für eine unidirektionale Filterung zuständig ist. Wählen Sie anschließend die Schnittstelle aus, auf der dieser Filter Anwendung finden soll. Zum Aktivieren bzw. Deaktivieren eines jeden Filters machen Sie vor den jeweiligen Filter einen Haken bzw. entfernen Sie den Haken.



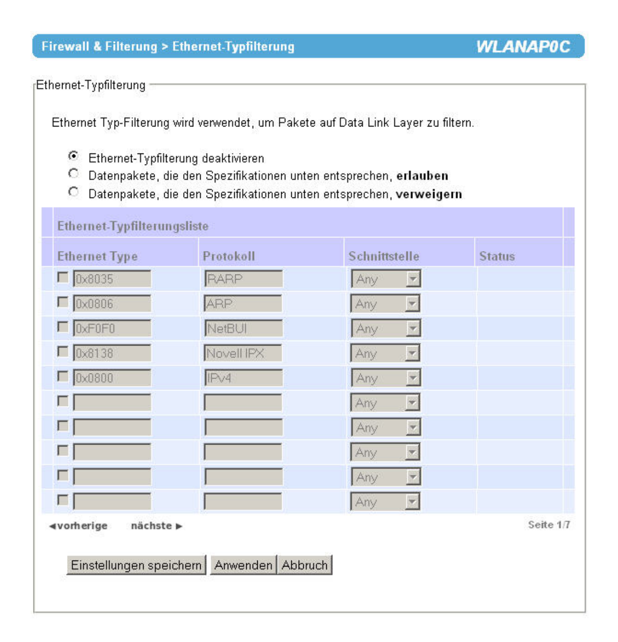
Filterung des IP-Netzwerk-Typs

8.7.4. Filterung des Ethernet-Typs

Mit der Filterung des Ethernet-Typs können Ethernetpakete auf der Grundlage ihres Typs zugelassen oder abgelehnt werden. Damit werden das Gerät und das dazugehörige Netzwerk vor einigen unerwünschten Paketen geschützt. Wählen Sie zum Aktivieren dieser Filterung „Only allow MAC Address [nur MAC-Adresse zulassen]“ oder „Only deny MAC Address [nur MAC-Adresse ablehnen]“ aus. Geben Sie anschließend den Ethernettyp und das Protokoll des Pakets ein, das sie zulassen oder ablehnen wollen. Wählen Sie anschließend die Schnittstelle aus, auf der dieser Filter Anwendung finden soll. Zum Aktivieren bzw. Deaktivieren eines jeden Filters (auf der Grundlage des Ethernet-Typs) machen Sie vor den jeweiligen Filter einen Haken bzw. entfernen den Haken.



Geben Sie zum Einrichten eines Filters des Ethernet-Typs „0x“ gefolgt von einer vierstelligen Hexadezimalzahl ein, beispielsweise 0xF0F0 um Nachrichten des Typs NETBUI zu filtern oder 0x8035, um Nachrichten des Typs RARP zu filtern.

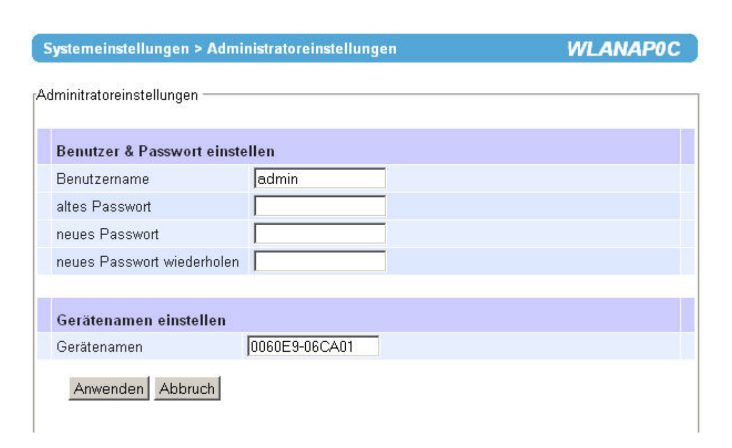


Filterung des Ethernet-Typs

8.8. Systemeinstellungen

8.8.1. Benutzer- und Passworteinstellungen

Die Benutzer- und Passworteinstellungen dienen zum Ändern des Benutzerkontos. Geben Sie zum Ändern des Administrator-Passworts als „Benutzername“ [User name] „admin“ und das Standardpasswort oder das alte Passwort ein, falls es geändert werden soll. Geben Sie in „Neues Passwort [New Password]“ anschließend ein neues Passwort ein und wiederholen Sie es in „Neues Passwort wiederholen [Repeat new password]“, um es zu bestätigen.

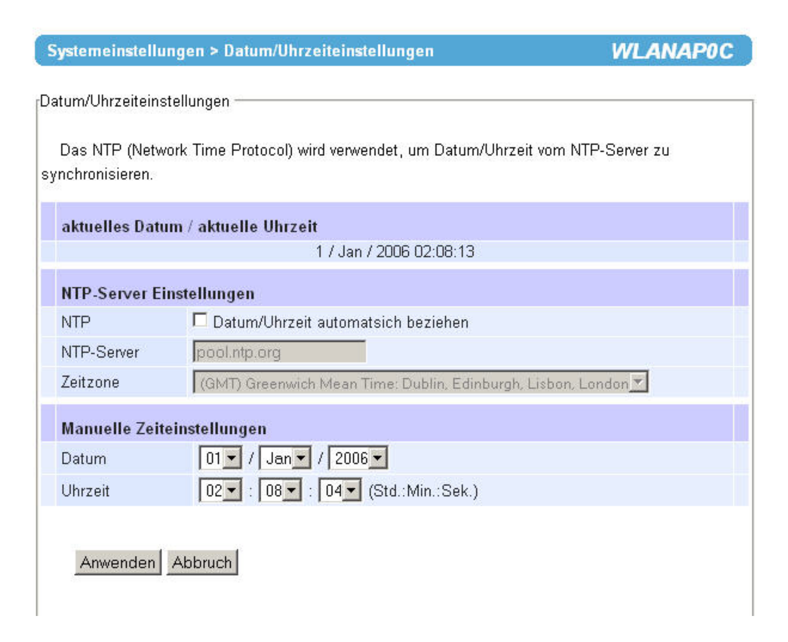


Benutzer- und Passworteinstellungen



8.8.2. Datum-/Uhrzeiteinstellungen

Datum und Uhrzeit sind für einige Funktionen des Geräts wichtig, die diese Angaben für den Betrieb benötigen. Sie können Datum und Uhrzeit des Geräts entweder manuell einstellen oder Sie können das Network Time Protocol (NTP) verwenden, um die Uhrzeit des Geräts mit einem Zeitserver zu synchronisieren. Machen Sie ein Häkchen bei „Obtain a date/time automatically [Datum/Uhrzeit automatisch beziehen]“ und geben Sie anschließend die IP-Adresse oder den Hostnamen eines NTP-Servers ein. Wenn Sie einen Hostnamen eingeben, muss der DNS-Server für dieses Gerät eingerichtet werden. Anschließend können Sie die Zeitzone des Geräts auswählen.



Datum- und Uhrzeiteinstellungen

8.8.3. Alarmereignis

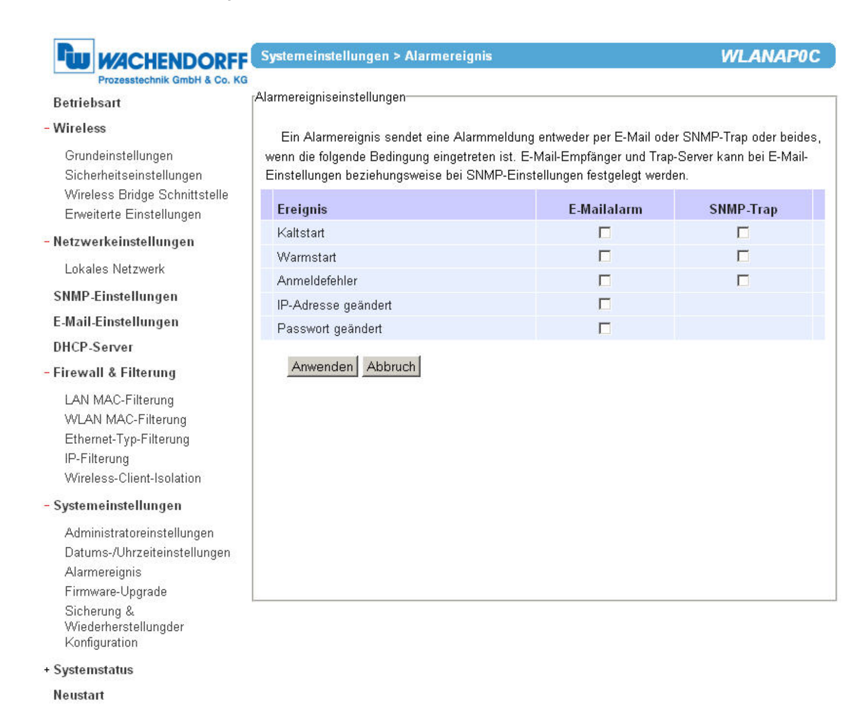
Es gibt fünf Ereignisse, bei denen das Gerät einen Alarm auslöst:

- Kaltstart (Bei Unterbrechung der Stromversorgung)
- Warmstart (Das Gerät wird über den Resetknopf neu gestartet)
- Authentifizierungsfehler (Der eingegebene Benutzername bzw. das eingegebene Passwort ist falsch)
- IP-Adresse wurde geändert (Die IP-Adresse des Geräts wurde geändert)
- Passwort geändert (Das Administrator-Passwort wurde geändert)

Jedes dieser Ereignisse stellt ein „Alarmereignis“ dar und bei seinem Eintreten müssen die jeweiligen verantwortlichen Mitarbeiter per E-Mail oder durch Einrichten einer Trap auf dem Trap-Server benachrichtigt werden. Informationen zum Einrichten der E-Mail-Adressen, an die die Alarmmeldung gesendet werden sollen, finden Sie im Abschnitt „E-Mail-Einstellungen“. Informationen zum Einrichten eines SNMP-Trap-Servers finden Sie im Abschnitt „SNMP-Einstellungen“.



Es können Alarmmeldungen aller Ereignisse in einer E-Mail versendet werden, aber nur die ersten drei Ereignisse können einen Trap des SNMP-Servers auslösen.



Alarmereignis-Einstellungen

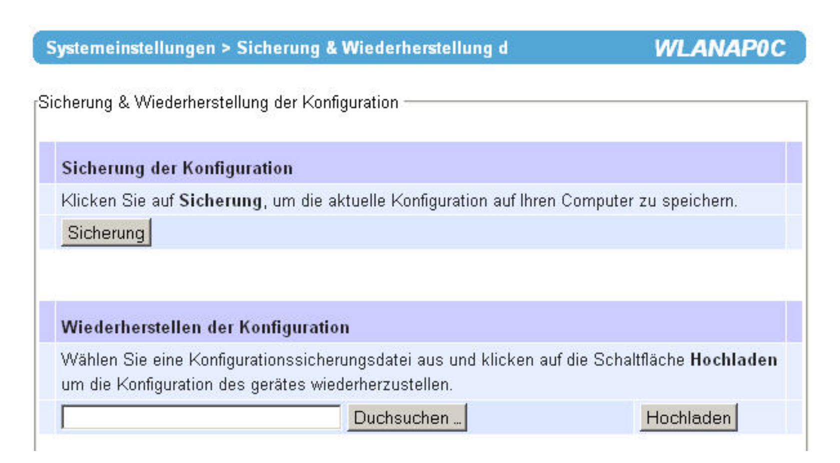
8.8.4. Konfiguration sichern und wiederherstellen

Wenn Sie alle Einstellungen abgeschlossen haben und das Gerät ordnungsgemäß funktioniert, können Sie Ihre Konfiguration sichern. Die Sicherungskopie kann verwendet werden, wenn die neue Firmware hochgeladen wird und auf die Werkseinstellungen zurückgestellt wird. Die Sicherungskopie kann außerdem zur Einrichtung anderer ähnlicher Geräte verwendet werden, ohne mehrere Konfigurationsschritte durchlaufen zu müssen.

Klicken Sie zum Erstellen einer Sicherungskopie Ihrer Konfiguration auf „Sicherungskopie [Backup]“; auf Ihrem Computer öffnet sich ein Pop-up-Dialog zum Speichern der Sicherungsdatei. Es ist wichtig, dass die gespeicherte Konfigurationsdatei NICHT durch einen Editor geändert wird. Jede Änderung kann die Datei beschädigen und sie zur Wiederherstellung untauglich machen.

Um die Sicherungskopie Ihrer Konfiguration wiederherzustellen klicken Sie auf „Durchsuchen [Browse]“, um die Sicherungsdatei zu finden und anschließend auf „Hochladen [Upload]“, um die Sicherungsdatei Ihrer Konfiguration auf das Gerät hochzuladen. Wenn die Sicherungsdatei Hochladeprozess erfolgreich hochgeladen wurde, führt das Gerät automatisch einen Neustart durch.





Konfiguration sichern und wiederherstellen



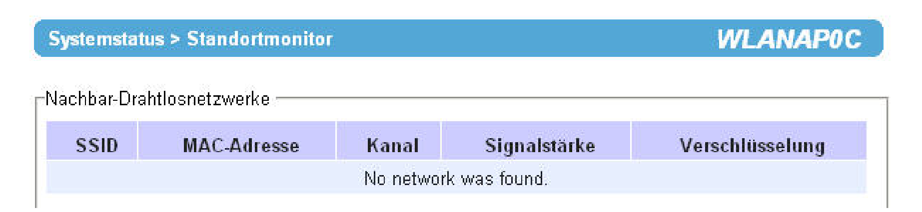
8.9. Systemstatus

Die Menüeinstellungen liefern die in den folgenden Abschnitten dargelegten Informationen über den Gerätestatus.

8.9.1. Site Monitor

Mit dem Site Monitor können Benutzer die anderen drahtlosen Netzwerke in den umgebenden Bereichen einsehen. Der Site Monitor zeigt Informationen über andere Access-Points an, wie zum Beispiel SSID, MAC-Adresse, verwendeter Kanal, RSSI (Received Signal Strength Indicator = empfangene Signalstärkeanzeige) und von den anderen Access-Points verwendetes Sicherheitsprotokoll. Der „Site Monitor" kann beim Einrichten der SSID und des Kanals dieses Geräts nützlich sein, um Kollisionen bei SSID-Namen und Kanal und unerwartete Fehler oder eine Leistungsminderung zu verhindern.

Die Funktion „Site Monitor" braucht eine gewisse Zeit, um Informationen über die umliegenden drahtlosen Netze zu sammeln.



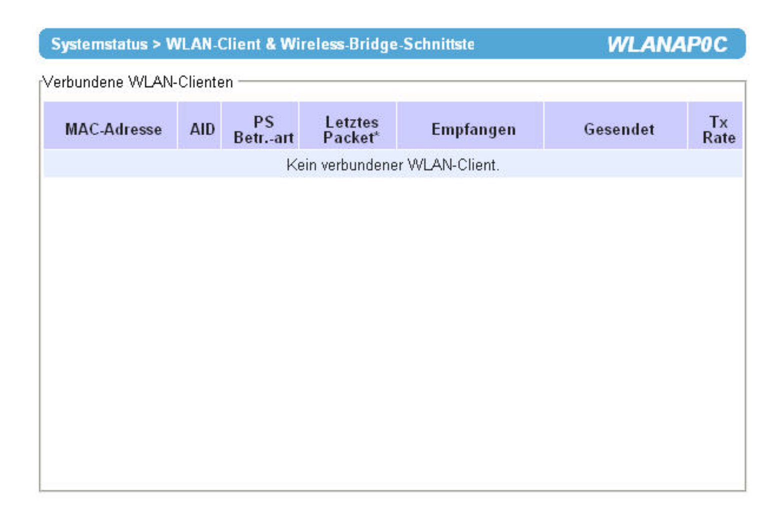
Snapshot des Site Monitors

8.9.2. Wireless Client und Wireless-Bridge-Schnittstelle

Der Administrator kann die Wireless-Clients, die auf diesen Access-Point oder auf andere drahtlose Netzwerke über die Wireless-Bridge-Schnittstellen zugreifen, nach verschiedenen Betriebsarten überwachen:

- Access-Point-Betrieb: Überwacht den Status der verbundenen Wireless-Clients. Die untere Abbildung zeigt die Informationen der verbundenen mobilen Clients an. Es werden die MAC-Adressen, die Anzahl der empfangenen und übertragenen Pakete sowie die Übertragungsrate der drahtlosen Verbindung angezeigt.
- Wireless-Betrieb: Überwacht den Status der anderen Netzwerke, die über eine Wireless-Bridge mit diesem Gerät verbunden sind. Untere Abbildung zeigt ein Beispiel für den Status eines anderen über eine Bridge verbundenen Netzwerks. Es wird die MAC-Adresse der Schnittstelle und die Anzahl der empfangenen und übertragenen Pakete sowie die aktuelle Übertragungsrate der drahtlosen Verbindung angezeigt.
- AP- + Wireless-Betrieb: Überwacht sowohl den Status der verbundenen Wireless Clients als auch der anderen über eine Bridge angeschlossenen Netzwerke.

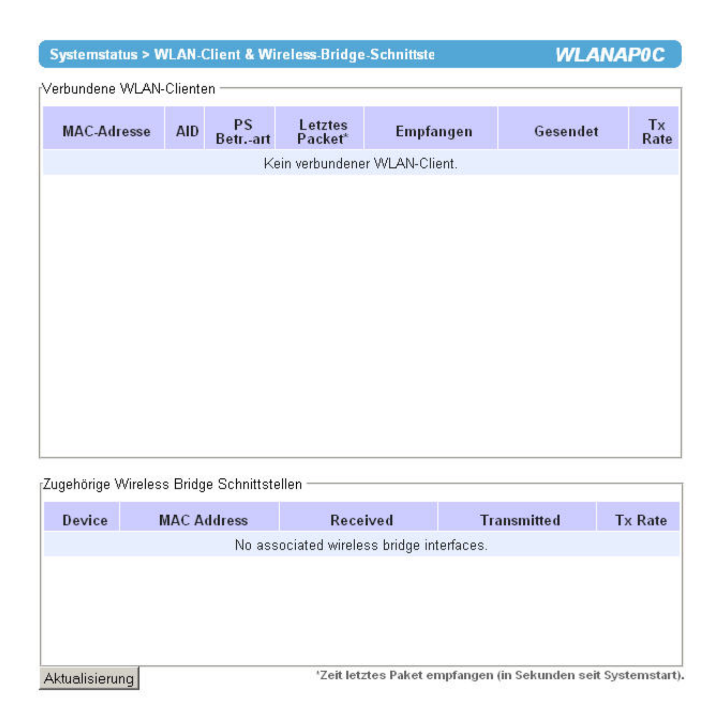




Die Wireless-Client-Tabelle zeigt den Status der Bridge-Schnittstelle an



Die Wireless-Bridge-Schnittstelle zeigt den Status des Bridge-Geräts an

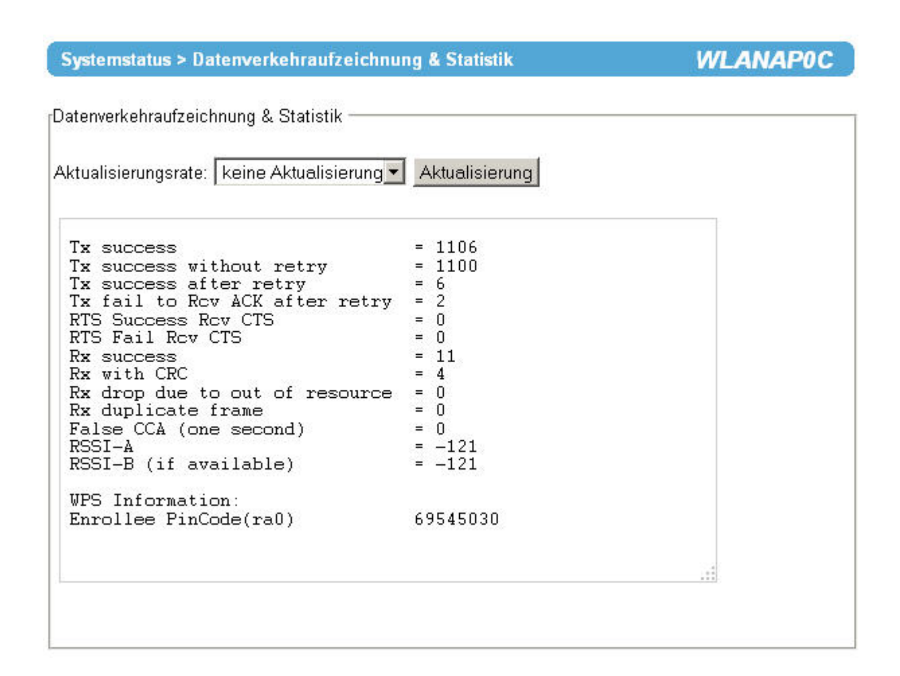


Die Wireless-Client- und Wireless-Bridge-Schnittstelle zeigt die kombinierten Informationen an



8.9.3. Traffic Log und Statistik

Unter „Traffic Log und Statistik“ werden Informationen über das drahtlose Netzwerk und über dessen Status angezeigt. Sie können die „Refresh Rate [Bildwiederholrate]“ der Traffic-Log-Anzeige einstellen. Standardmäßig ist sie auf 30 Sekunden eingestellt. Eine hohe Bildwiederholrate würde die CPU-Last Ihres Geräts erhöhen.

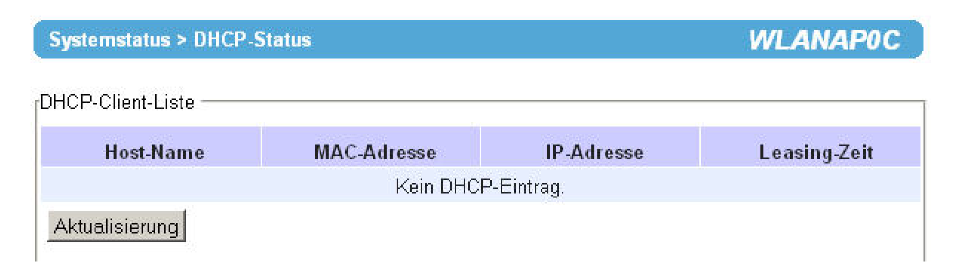


Traffic Log und Netzwerkstatistik



8.9.4. DHCP-Status

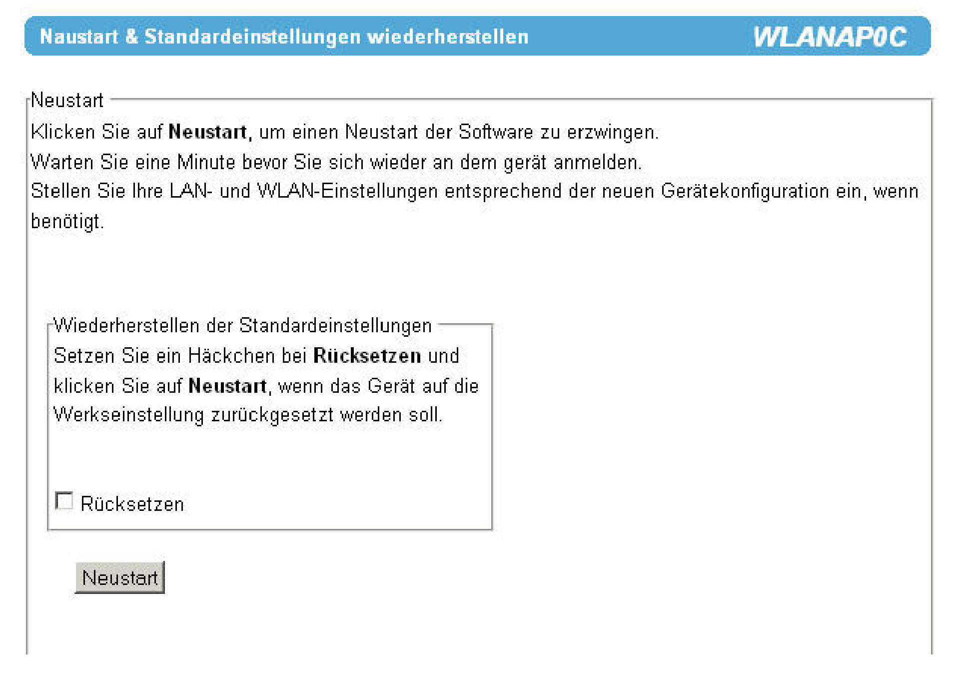
Der DHCP-Status zeigt die Liste der DHCP-Clients, die von diesem Gerät IP-Adressen empfangen, wenn das Gerät die IP-Adressen per DHCP-Protokoll verteilt. Die Liste zeigt MAC-Adressen, IP-Adressen, Typ und Status von Mobilstationen.



DHCP-Status Snapshots

8.10. Neu starten und Standardeinstellungen wiederherstellen

Um das Gerät manuell neu zu starten, klicken Sie auf „Reboot [Neu starten]“ und das Gerät wird neu gestartet. In einigen Fällen wollen Sie das Gerät unter Umständen wieder auf die Werkseinstellungen zurückstellen. Kreuzen Sie dazu das Kästchen „Reset“ an und klicken Sie anschließend auf „Neu starten“ [Reboot], um Ihr Gerät mit den Werkseinstellungen neu zu starten.



Neu starten und Standardeinstellungen wiederherstellen



9. Spezifikationen

Hardwarespezifikationen

CPU	150 MHz RISC mit MMU-Unterstützung
Flash-Speicher	8 MB für Programme und Daten 2MB für Bootloader
RAM-Speicher	SDRAM: 32 MB
Interne Schnittstelle	Mini-PCI Slot (für Wireless-Modul)
Watchdog	Hardware Watchdog Reset
Diagnoseschnittstelle	RS232
Wireless LAN	FCC-zertifiziertes IEEE 802.11 b/g 802.11b Datenübertragungsraten: 11/5.5/2/1 Mbps 802.11g Datenübertragungsraten: 54/48/36/24/18/12/9/6/5.5/2/1 Mbps Betriebskanäle: 802.11b/g: 11 (Nordamerika), 13 (Europa), 14 (Japan) Sicherheit: WEP, WPA, WPA2, TKIP, AES, 802.1x WEP-Verschlüsselungslänge: 64 Bit und 128 Bit Tx Power 11b: 14 dBm, 11g: 13 dBm Rx-Empfindlichkeit: -66 dBm bei 54 Mbps, -80 dBm bei 11Mbps 802.11b/g Außenbereich: 980 Fuß / 300 m Antennenanschluss: Reverse SMA Topologien: Infrastruktur
Ethernet	802.3u 10/100 BaseTX Ethernet LAN Schutz: Eingebaute 1,5 kV magnetische Isolierung
Spannungsversorgung	Eingang: DC 24V - 48V Verbrauch: 4,5 W bei Tx-Modus
Abmessungen	H x B x T: 90 mm x 45 mm x 75 mm
Temperaturen	Betrieb: 0 bis 60 C, 5 bis 95% RH Lagerung: -40 bis 70 C, 5 bis 95% RH
Antenne	2 dBi Antenne



Softwarespezifikationen

Protokolle	HTTP, DHCP, TCP/IP, RADIUS, DNS, SNMP, NTP
Erweiterte Funktionen	Fast Handoff, Smart Route, Wireless Client Isolation, Advanced Firewall und Paketfilterung,
Konfiguration	Web-basierte Verwaltung
Client OS-Unterstützung	Windows 95/98/2000/ME/NT/XP, UNIX und Macintosh
Antenne	2 dBi
Wireless Security	AP-STA: OPEN/WEP/WPA/WPA2/RADIUS WDS: Open, WEP, TKIP, CCMP(AES) Verschlüsselungsalgorithmus

LED-Anzeigen

Name	Farbe	Bedeutung
Access Point	● (Leuchtet dauerhaft Grün)	Access-Point-Betrieb
Wireless Bridge	● (Leuchtet dauerhaft Grün)	Wireless-Bridge-Betrieb
AP + Wireless Bridge	● (Leuchtet dauerhaft Grün)	„AP + Wireless Bridge"-Betrieb
BELEGT	● (Dauerhaft AUS)	RESERVED LED, keine Funktion
WLAN	(Blinkt Grün)	Laufender Datenverkehr über die WLAN-Schnittstelle
LAN	(Blinkt Grün)	Laufender Datenverkehr über die LAN-Schnittstelle
RUN	(Blinkt Grün)	Gerät ist in Betrieb
Power	● (Leuchtet dauerhaft Grün)	Gerät ist EIN geschaltet



Kundenservice und Technischer Support

Bei technischen Problemen & Fragen erreichen Sie uns unter Tel. +49 – (0) 6722 – 9965 - 966

Schauen Sie auf unserer Homepage oder wenden Sie sich an uns über E-Mail:

web: www.wachendorff-prozesstechnik.de
mail: eea@wachendorff.de

Bestellhinweise

Typ	Bestell-Nr.
WLAN Access Point Compact IEEE802.11 g/b Aufschraubbare Demo-Whip Antenne 2 dBi im Lieferumfang enthalten	WLANAP0C
Zubehör:	
WLAN Client Adapter IEEE802.11 g/b	WLANCL00
Standard-Dipolantenne 2,4GHz@4dBi	WLANANT55
Hochleistungsantenne Stabantenne 2,4GHz@9dBi m. 1,5 m Kabel	WLANANT90
Hutschienen-Schaltnetzteil 230V/24VDC	PS24V03AA